



NOTE

Against Geofences

Haley Amster & Brett Diehl*

Abstract. Law enforcement is increasingly relying on a new tool when investigating crimes with no suspects: geofence warrants. Geofence warrants take advantage of geofence technology, which constructs a virtually bounded geographic area and identifies all users present within that area during a given time window. Google, the primary recipient of geofence warrants, has adopted a policy of objecting to any geofence request that is not a probable-cause warrant. So far, law enforcement has complied. This has caused courts and litigators to defer the question of whether, under *Carpenter v. United States*, a probable-cause warrant is necessary. Instead, these parties have located the legality of geofence warrants in less explored regions of the Fourth Amendment as applied to new technologies: probable-cause and particularity requirements, the few exceptions to those requirements, and the proper execution of a warrant.

This Note fills an analytical void by providing a comprehensive examination of these less explored regions. The Note first provides a technology primer, detailing the three steps involved in geofence warrants: the initial data dump, selective expansion, and unmasking. It then provides background on relevant Fourth Amendment law, explaining why the familiar “reasonable expectation of privacy” test has not yet proven dispositive in geofence-warrant litigation. After cataloguing burgeoning geofence litigation, the Note examines the initial data dump, identifying the difficulty of meeting probable-cause and particularity requirements due to the inherent breadth of the search. Here the Note

* Haley Amster is a law clerk at Covington & Burling LLP; J.D., Stanford Law School, 2021. Brett Diehl is a trial attorney at Federal Defenders of San Diego, Inc.; J.D., Stanford Law School, 2021.

Our deepest gratitude to Robert Weisberg for his encouragement, guidance, and insights. Thanks to Michael W. McConnell, Morgan N. Weiland, and the rest of the Constitutional Law Center for their support and guidance. Thanks to Jonathan Abel, David Sklansky, Jonathan Mayer, Orin Kerr, John Ellis, Rick Salgado, Todd Hinnen, Sierra Villaran, Laura Koenig, the participants of the Constitutional Law Center’s Works-in-Progress Workshop, and the students of the Legal Studies Workshop for their helpful comments and feedback throughout the drafting process. Thanks to editors and friends—Marty Berger, Marc Brunton, Julia Irwin, Jenny Jiao, Dan Kim, Matt Krantz, David Levin, Caro Sundermeyer, Daphne Thompson, Mitchell Wong, Jeffrey Xia, and Peggy Xu—who made this Note better with their insightful edits and commentary. And thanks to Tal Klement for immediately recognizing the many questions that geofence warrants raise. All views expressed are our own and do not reflect those of any current or former employers.

answers the question of whether probable cause must be shown for each device included in a digital search, based in part on jurisprudence regarding checkpoints, area warrants, and searches of many people in a commercial location. The Note next examines the selective expansion and unmasking steps, arguing (1) that geofence warrants are unconstitutional general warrants because of the discretion given to law-enforcement officials in warrant execution; and (2) that these steps may impermissibly increase a warrant's scope or constitute multiple searches under one warrant. The Note concludes by considering the broader implications of corporate policy shaping Fourth Amendment guardrails.

Table of Contents

Introduction	388
I. The Technology Behind a Geofence Request.....	393
A. The SensorVault.....	394
B. Warrant Execution	398
1. Initial data dump.....	399
2. Selective expansion	404
3. Unmasking.....	405
II. Geofences and the Fourth Amendment.....	406
A. Is a Geofence a Fourth Amendment “Search”?.....	406
B. Probable Cause, Particularity, and Warrant Execution	410
III. How Courts Are Handling Geofence Warrants	411
A. Northern District of Illinois Magistrate Opinions	412
1. Pharmaceutical sale investigation: first denial.....	413
2. Pharmaceutical sale investigation: second denial	414
3. Pharmaceutical sale investigation: third denial.....	415
4. Arson investigation.....	416
B. District of Kansas Magistrate Opinion.....	417
C. Ongoing State and Federal Litigation	419
D. Preliminary Takeaways from the Early Litigation.....	421
IV. Constitutionality of the Initial Data Dump.....	422
A. Probable Cause.....	422
1. Geofences as <i>Ybarra</i> searches	423
2. Geofences as checkpoints.....	425
3. Geofences as area warrants	427
4. Takeaways.....	429
B. Issues with the Particularity Requirement.....	431
V. Constitutionality of Selective Expansion and Unmasking	433
A. Geofences as General Warrants	433
B. Selective Expansions as Increases in Scope	435
C. Multiple Searches.....	436
VI. Corporate Policy and Fourth Amendment Protections.....	437
A. Absence of Legislation	438
B. Corporate Constitutional Policy	440
Conclusion.....	444

Introduction*

Suppose a law-enforcement officer investigating a hit-and-run sets up a checkpoint near the site of the incident. The investigating officer stops each passerby and examines their cell phone location history to determine if they were present at the crime scene. This officer would be in violation of the Fourth Amendment for employing a checkpoint in the “ordinary enterprise of investigating” a crime.¹ Now suppose that officer obtains a warrant compelling Google to do the same thing—digitally. Different result?²

Since roughly 2016, law enforcement has used geofence warrants to help revive criminal investigations gone cold.³ These warrants have become increasingly common,⁴ and there are even indications that a warrant-authorized geofence was used to investigate the January 6, 2021 attempted insurrection at the U.S. Capitol.⁵

Geofence warrants “work in reverse” from traditional search warrants.⁶ Instead of law enforcement requesting that a third-party provider produce the location history of a particular suspect’s device, geofence warrants proceed first by giving investigators access to data for all cellular devices that were present near a crime scene around the time when the crime occurred. Through a series

* This Note is current as of November 2021. Subsequent changes in the legal landscape are not addressed.

1. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 44, 48 (2000) (invalidating a checkpoint employed “primarily for the ordinary enterprise of investigating crimes”); cf. *Illinois v. Lidster*, 540 U.S. 419, 423, 427–28 (2004) (upholding a checkpoint because its primary purpose was not to “determine whether a vehicle’s occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others”).
2. Credit is due to Dennis Martin for inspiring our introduction. See Dennis Martin, Note, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 693 (2018).
3. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), <https://perma.cc/P75R-DZCU> (to locate, select “View the live page”). We use “geofence warrant” to align with the term most commonly used by litigators and commentators. See, e.g., *id.* But the precise term is “reverse location” warrant. See, e.g., Thomas Brewster, *To Catch a Robber, the FBI Attempted an Unprecedented Grab for Google Location Data*, FORBES (Aug. 15, 2018, 9:00 AM EDT), <https://perma.cc/XG3N-JEGG>; Tyler Dukes, *To Find Suspects, Police Quietly Turn to Google*, WRAL.COM (Mar. 15, 2018, 5:05 AM), <https://perma.cc/RFU9-XDF7>.
4. Alfred Ng, *Privacy Groups Demand Google Disclose Details on Geofence Warrants*, CNET (Dec. 8, 2020, 5:00 AM PT), <https://perma.cc/TGS4-DUE5>.
5. Statement of Facts at 5–6, *United States v. Groseclose*, No. 21-mj-00250 (D.D.C. Feb. 22, 2021), 2021 U.S. Dist. Ct. Pleadings LEXIS 132, ECF No. 1-1; Drew Harwell & Craig Timberg, *How America’s Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM EDT), <https://perma.cc/Q257-LHYT>.
6. Sidney Fussell, *Creepy “Geofence” Finds Anyone Who Went Near a Crime Scene*, WIRED (Sept. 4, 2020, 7:00 AM), <https://perma.cc/Y3S8-ZT8Q>.

of iterative steps between the provider and law enforcement—without the further involvement of a magistrate judge—the provider produces additional location data with the goal of (1) helping law enforcement figure out which devices could have been those of the perpetrators; and (2) ultimately revealing the identities of the suspects.

Such sweeping searches can unearth the location history of a startling number of users. One 2019 geofence warrant authorized a geofence covering a total of 29,387 square meters (or 7.4 acres—about the size of five and a half American football fields) over a period of nine hours.⁷ In response, the provider returned to law enforcement the location data of 1,494 cell phones.⁸

So far, Google has been the primary recipient of geofence warrants. This is in large part due to Google's location-history database, the SensorVault. Google uses the SensorVault to target advertisements, determine when stores are busy, help users track their movements, and provide traffic estimates.⁹ But law-enforcement officials now also use the SensorVault for criminal investigations. In response to increasing government requests for information, Google has crafted a three-step, self-directed process for law-enforcement officials trying to obtain user data. As Google explained in a 2020 court filing, it has "instituted a policy of objecting to any warrant that fail[s] to include" its mandated tailoring process.¹⁰

In recent years, the number of SensorVault-directed geofence warrants has grown rapidly. According to data released by Google, geofence warrants "recently constitut[ed] more than 25% of all [U.S.] warrants" received by the company.¹¹ Google disclosed that it received 982 geofence-warrant requests in

7. Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented "Geofence" Search*, FORBES (Dec. 11, 2019, 7:45 AM EST), <https://perma.cc/34QP-XMKY>.

8. *Id.*

9. See Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works*, N.Y. TIMES (Apr. 13, 2019), <https://perma.cc/FPL9-KRX6>; Declaration of Marlo McGriff ¶ 26, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-1. For example, if a cell phone owner is walking toward a Starbucks, she might see a Starbucks coupon appear on her device (because her device sensed that she was near the store). Once she goes into the Starbucks and uses her coupon, her device registers that information. Google tracks and stores such advertisement-servicing and usage data.

10. Declaration of Sarah Rodriguez ¶ 5, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-2.

11. Google, Supplemental Information on Geofence Warrants in the United States 1 (n.d.), <https://perma.cc/6B34-PPCX>. A TechCrunch article notes that Google released this data in August 2021. See Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021, 2:54 PM PDT), <https://perma.cc/V95P-2MMD>.

2018.¹² This figure, Google explained in a court document, represented “over a 1,500% increase in the number of geofence requests . . . [as] compared to 2017.”¹³ In 2019, the number of geofence warrants received by Google increased by a further 755% over the previous year to 8,396.¹⁴ In 2020, the last year for which specific statistics are publicly available at the time of writing, Google received 11,554 geofence warrants.¹⁵ California law enforcement represents the most frequent geofence-warrant requester, having submitted 3,655 of the 20,932 requests logged by Google over the three-year period.¹⁶ Texas law enforcement came in second with 1,825 geofence warrants submitted to Google.¹⁷ By contrast, federal law enforcement submitted only 928 requests from 2018 to 2020.¹⁸

As geofences become more well-known, at least one crime victim’s family has specifically urged investigators to request a geofence warrant.¹⁹ The Department of Justice’s Computer Crimes and Intellectual Property Section has held discussions with Google about geofences and, in at least one instance, provided a boilerplate geofence-warrant request form to an FBI agent.²⁰ Hawk Analytics, which frequently assists law-enforcement investigations across the country,²¹ hosted a webinar for law enforcement called “Working with Google Geofence Reverse Location Search Records” and previously offered an online tool allowing investigators to obtain a “Google geofence warrant in a few

12. Google, *supra* note 11, at 2 (to locate, select “View the live page,” and then select “Download supplemental data as a CSV”).

13. Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant’s Motion to Suppress Evidence from a “Geofence” General Warrant (ECF No. 29) at 3, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 20, 2019), 2019 WL 8227162, ECF No. 59-1 [hereinafter Google Amicus Brief].

14. Google, *supra* note 11, at 2 (to locate, select “View the live page,” and then select “Download supplemental data as a CSV”).

15. *Id.*

16. *Id.*

17. *Id.*

18. *Id.*

19. Shannon Ryan, *Family, Investigators Push for Geofence Warrant in Jason Landry Case*, FOX 7 AUSTIN (May 11, 2021), <https://perma.cc/NX7G-4FLK>.

20. Mr. Chatrie’s Post-hearing Brief on “Geofence” General Warrant at 3-4, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. May 3, 2021), ECF No. 205 [hereinafter *Chatrie* Post-hearing Brief].

21. Sam Richards, *Powerful Mobile Phone Surveillance Tool Operates in Obscurity Across the Country*, INTERCEPT (Dec. 23, 2020, 6:31 AM), <https://perma.cc/57XS-WX2X>.

‘clicks.’”²² Reports of wrongful arrests due to geofence warrants have already emerged.²³

Courts and legislatures have paid little attention to how the Fourth Amendment applies to geofence warrants.²⁴ This is largely due to the novelty of the tool: As of this writing, most litigation has been *ex parte*, only five magistrate opinions considering the issue have been unsealed, and some of the first state and federal challenges by criminal defendants are underway.²⁵ But the lack of attention may also be due to Google’s unique role. Since the Supreme Court’s landmark decision in *Carpenter v. United States*—holding that the production of seven days’ worth of cell phone location information constitutes a Fourth Amendment search requiring a warrant²⁶—litigation and scholarship have focused on whether non-*Carpenter* technologies also lead to

22. *Working with Google Geofence Reverse Location Search Records*, HAWK ANALYTICS (Jan. 23, 2020), <https://perma.cc/3QQ4-HAXM>; Hawk Analytics (@hawkanalytics), FACEBOOK (June 17, 2019) (capitalization altered), <https://perma.cc/LD5J-QDNY> (to locate, select “View the live page”); Johana Bhuiyan, *The New Warrant: How US Police Mine Google for Your Location and Search History*, GUARDIAN (Sept. 16, 2021, 6:00 AM EDT), <https://perma.cc/94H4-ERPF>.

23. See *infra* notes 57–67 and accompanying text.

24. See *infra* Parts III, VI.A. And the literature has only begun to explore the many questions raised by this new tool. See Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2515–20 (2021) (considering the question of when a geofence search occurs and arguing that it occurs when the provider searches its database, not when law enforcement receives the requested data); Tim O’Brien, *Suspicionless Search: Geofence Warrants and the Fourth Amendment* 19–31 (Aug. 6, 2021) (unpublished manuscript), <https://perma.cc/L7C3-SYZ3> (highlighting the shortcomings of anonymization in the geofence-warrant process and arguing that Fourth Amendment case law and statutory protections are insufficient to protect users’ privacy); Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, CRIM. JUST., Summer 2020, at 7, 12–13 (recommending limitations on the use of geofence warrants, such as allowing these warrants only for violent offenses and only after exhausting traditional investigation methods). See generally John C. Ellis, Jr., *Google Data and Geofence Warrant Process*, NLSBLOG.ORG (Jan. 8, 2021), <https://perma.cc/E7CW-7NZJ> (explaining geofence-warrant technology and execution); Nathaniel Sobel, *Do Geofence Warrants Violate the Fourth Amendment?*, LAWFARE (Feb. 24, 2020, 1:03 PM), <https://perma.cc/Y4MV-FTVR> (detailing the motion to suppress filed in *United States v. Chatrue*, a case discussed below). This Note breaks new ground by focusing on how to properly conduct the probable-cause inquiry, explaining that courts must focus the inquiry on each device swept up in the geofence search. This Note also makes a novel contribution by introducing analogies to checkpoints, area warrants, and searches of many people in a commercial location. Finally, this Note is the first to highlight the broader impacts of Google’s role in this emerging issue, arguing that the corporation’s policies have played an outsized role in shaping law-enforcement norms and practices.

25. See *infra* Part III.

26. 138 S. Ct. 2206, 2212, 2217 n.3, 2220–21 (2018).

Fourth Amendment searches.²⁷ For geofences specifically, however, Google's policy of objecting to any request not derived from a probable-cause warrant has deferred the familiar "is this a Fourth Amendment search" question.²⁸ Questions surrounding geofence warrants' legality thus occupy less explored regions at the intersection of new technology and the Fourth Amendment: probable cause, particularity, and proper warrant execution.

This Note fills an analytical void by providing a comprehensive examination of these underexplored Fourth Amendment warrant requirements. It proceeds in six parts. Part I is a technology primer, detailing the three steps involved in geofence warrants: the initial data dump, selective expansion, and unmasking. Part II provides a background of relevant Fourth Amendment doctrine, including a discussion of how *Carpenter* intersects with geofence warrants. Part III catalogs burgeoning geofence litigation, with a special focus on the first few federal magistrate opinions on the issue. Part IV considers the initial data dump, identifying the difficulty of meeting probable-

27. See *id.* at 2220 (noting the decision's narrow scope). For post-*Carpenter* litigation, see generally *United States v. Moore-Bush*, 963 F.3d 29 (1st Cir.) (holding that *Carpenter* does not extend to eight months of video surveillance conducted using a pole camera), *vacated and reh'g en banc granted*, 982 F.3d 50 (1st Cir. 2020); *State v. Sylvestre*, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018) (holding that *Carpenter* extends to cell-site simulator location data); and *United States v. Diggs*, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that *Carpenter* extends to the acquisition of a vehicle's long-term GPS data). For post-*Carpenter* scholarship applying the decision in a variety of contexts, see, for example, Orin S. Kerr, *Implementing Carpenter* (USC L. Legal Stud. Working Paper, Paper No. 18-29, 2018), <https://perma.cc/XG96-NMTR> (arguing that *Carpenter* should apply to non-content internet records if those records are collected by new digital technologies, are collected without a user's meaningful consent, and reveal intimate personal details); Susan Freiwald & Stephen Wm. Smith, *The Supreme Court, 2017 Term—Comment: The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 227-31 (2018) (suggesting *Carpenter* may extend to real-time location information, fewer than seven days of historical location information, and other technologies); Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), <https://perma.cc/A2SX-Z9GP> ("[A]lmost everything we do in the digital age—social media, internet searches, the Internet of Things—has locational privacy implications because they track location, and *Carpenter* suggests that they might also have Fourth Amendment implications."); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 375-76 (2019) (suggesting that *Carpenter* could extend to real-time location information); Lara M. McMahon, Note, *Limited Privacy in "Pings": Why Law Enforcement's Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment*, 77 WASH. & LEE L. REV. 981, 1027 (2020) (arguing that *Carpenter* does not extend to all cell phone pings); Emma Lux, Student Contribution, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. ONLINE 109, 113-18 (2020) (analyzing whether *Carpenter* extends to tower dumps); and Stephanie Foster, Note, *Should the Use of Automated License Plate Readers Constitute a Search After Carpenter v. United States?*, 97 WASH. U. L. REV. 221, 238-39 (2019) (asserting that *Carpenter* extends to aggregated data from automated license-plate readers).

28. See *infra* Part II.A.

cause and particularity requirements due to the inherent breadth of the search. Here the Note analogizes to the search of many people located at the scene of a crime in *Ybarra v. Illinois*,²⁹ the use of digital checkpoints, and the use of area warrants. It then explores the difficulty of tailoring by (1) examining digital searches of multi-occupancy buildings; (2) surveying scholarship and litigation regarding tower dumps; and (3) suggesting particularized search protocols that could meet constitutional requirements. Part V examines the selective expansion and unmasking steps, arguing that geofence warrants are unconstitutional general warrants because of the discretion given to law-enforcement officials in warrant execution. Part V also argues that the selective-expansion and unmasking steps may impermissibly increase a warrant's scope or constitute multiple searches under one warrant. Finally, Part VI considers the broader implications of corporate policy driving Fourth Amendment guardrails.

I. The Technology Behind a Geofence Request

A geofence warrant compels Google to produce data from its SensorVault location-history database.³⁰ Under Google's threat of noncompliance, most geofence warrants proceed in three steps: the initial data dump, selective expansion, and unmasking. This Part first explains the SensorVault and then elaborates on each of the three execution steps, drawing on unsealed search warrants from federal and state investigations as examples.

29. 444 U.S. 85, 87-88 (1979).

30. See Valentino-DeVries, *supra* note 3 ("Investigators who spoke with The New York Times said they had not sent geofence warrants to companies other than Google, and Apple said it did not have the ability to perform those searches."). Google is the only company known to release location-history data in this manner. Leila Barghouty, *What Are Geofence Warrants?*, MARKUP (Sept. 1, 2020, 8:00 AM ET), <https://perma.cc/XQ3Z-K88H>. Microsoft recently stated that it "does not and would not be in a position to comply with any warrants seeking such [location] information." *Id.* (quoting Microsoft Assistant General Counsel Hasan Ali). Facebook stated that it does not fulfill geofence warrants because of its less precise location information and limitations on data storage. David Uberti, *Police Requests for Google Users' Location Histories Face New Scrutiny*, WALL ST. J. (July 27, 2020, 5:30 AM ET), <https://perma.cc/C9DM-SS9E>. Lyft has signaled a potential willingness to fulfill geofence warrants if undefined specificity conditions are met. *Id.* Garmin has stated that it would not fulfill geofence warrants if served because of a belief that such requests are "invasive of our users' privacy rights." *Id.* (quoting a Garmin representative). Amazon Web Services recently announced that it will add "Amazon Location" geofence capabilities for companies hosted on its platform. Renato Losio, *AWS Introduces Location Service in Preview*, INFOQ (Jan. 3, 2021), <https://perma.cc/S2K6-5PU4>.

A. The Sensor Vault

Google's SensorVault is a prodigious pool of consumer location information, pioneered in part to target advertisements but now routinely used by law enforcement for geofence warrants.³¹ Cell-service providers and other corporations also collect cell-site location information for various purposes.³² Yet the SensorVault and linked internal Google databases are more expansive, storing user location information generated from "search queries," "users' IP addresses, device sensors," and "device signals including GPS, information cellular networks provide to a device, information from nearby Wi-Fi networks, and information from nearby Bluetooth devices."³³ Multiple inputs can be combined to estimate a user's location "to a high degree of precision."³⁴ Google refers collectively to this data, regardless of its source, as location history (LH). Absent a user request or account closure, LH is stored within Google's databases for at least eighteen months.³⁵

Google's LH practices affect the vast majority of people living in the United States. Eighty-five percent of Americans currently own a smartphone

-
31. See *supra* note 9 and accompanying text. For examples of commercial uses of location data, see *Geofencing Advertising Platform*, GROUNDTRUTH, <https://perma.cc/MWE6-DUCL> (archived Oct. 22, 2021); Sarah Berry, *Geofencing Marketing: The New Way to Market Your Business*, WEBFX (Apr. 20, 2021), <https://perma.cc/4MKB-RYK8>; and Justin Croxton, *Geofencing Advertising: What Is Geo Fencing & How Does It Work*, PROPELLANT MEDIA (Jan. 5, 2021), <https://perma.cc/CDP6-NTAM>. The use of location data and geofences to target advertisements raises privacy and ethics questions beyond the scope of this Note. See, e.g., Kearston L. Wesner, *Is the Grass Greener on the Other Side of the Geofence? The First Amendment and Privacy Implications of Unauthorized Smartphone Messages*, 10 CASE W. RES. J.L. TECH. & INTERNET, no. 1, 2019, at 1, 1-3 (describing a settlement regarding geofence-based advertisements that targeted women in the vicinity of abortion clinics and encouraged them not to terminate their pregnancies); John G. Browning, *Geo-Fencing: Free Speech or Tainting the Jury Pool?*, J.L. & TECH. TEX. (Nov. 15, 2019), <https://perma.cc/9EVH-F7RK> (describing Monsanto's use of geofences to target ads highlighting its herbicide's safety in the lead-up to a California trial on the issue).
32. See *supra* note 31; see also, e.g., AT&T, AT&T Location Information Services 1-2 (2012), <https://perma.cc/8E5N-FV4C>.
33. Exhibit 202 at 4, State v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. July 17, 2020); see also Google Amicus Brief, *supra* note 13, at 10 ("[I]nputs include not only information related to the locations of nearby cell sites, but also GPS signals . . . or signals from nearby Wi-Fi networks or Bluetooth devices.").
34. Google Amicus Brief, *supra* note 13, at 10. Google's geofence-warrant results normally include an indication of location precision, shown via a radius in which Google's algorithm has calculated the user is likely located. A smaller radius, resulting from more location inputs or better quality, indicates a more precise location. See *infra* Figure 3; *infra* notes 73-74 and accompanying text.
35. See Jessica Bursztynsky, *Google Just Announced It Will Automatically Delete Your Location History by Default*, CNBC (updated June 24, 2020, 12:11 PM EDT), <https://perma.cc/RN7M-6XQF>.

with mobile internet capabilities.³⁶ Approximately 46.8% of these U.S. smartphones operate on Google's Android operating system.³⁷ Across platforms, three of the five most popular smartphone applications in the United States—Gmail, Google Maps, and Google Search, each accessed on over 50% of U.S. smartphones—belong to Google.³⁸ And for the over 220 million estimated U.S. mobile search users,³⁹ 96% of searches were conducted via Google as of the first quarter of 2020.⁴⁰ Google's servers capture location data from all of these services: the Android operating system, Google-owned mobile applications, and in-browser mobile searches via Google.⁴¹

Presumably because of its vast information troves, Google is receiving geofence-warrant requests at an alarming rate. Google publishes the aggregate figures for subpoenas, court orders, warrants, and other requests that it receives from U.S. law enforcement, but until recently it did not release specific geofence-warrant tallies.⁴² In 2019, an anonymous Google employee told the *New York Times* that the corporation received upwards of 180 geofence warrants in one week.⁴³ In January 2020, in what experts speculated could be a tactic to deter law-enforcement requests, Google began charging \$245 for

36. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), <https://perma.cc/5UX9-P7PU>.

37. S. O'Dea, *U.S. Smartphone Subscriber Share by Operating Platform 2012-2021, by Month*, STATISTA (Aug. 11, 2021), <https://perma.cc/3KRQ-TS53> (to locate, select "View the live page").

38. See Statista Rsch. Dep't, *Reach of Most Popular U.S. Smartphone Apps 2021*, STATISTA (July 26, 2021), <https://perma.cc/9MVQ-K8QC> (to locate, select "View the live page"). A fourth, YouTube, is owned by Google's parent company, Alphabet. See *id.*

39. Statista Rsch. Dep't, *Number of Mobile Search Users in the United States 2014-2020*, STATISTA, <https://perma.cc/PV5B-3VWZ> (archived Oct. 22, 2021) (to locate, select "View the live page").

40. Joseph Johnson, *U.S. Total & Mobile Organic Search Visits 2020, by Engine*, STATISTA (Feb. 22, 2021), <https://perma.cc/43LF-PNRW>.

41. See *How Google Uses Location Information*, GOOGLE, <https://perma.cc/D4ZX-C9A3> (archived Oct. 22, 2021). The government has explained the ubiquity of Google products in court filings. "In its affidavit, the government asserts that approximately 97% of smartphones in the world use Google applications or Google's operating system," which would allow those smartphones to appear in a geofence if present within its boundaries. *In re the Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-00297, 2020 WL 5491763, at *3 (N.D. Ill. July 8, 2020). "[T]he government asserts a likelihood 'that at any given time, a mobile telephone, regardless of make, is interfacing in some manner with a Google application, service, and/or platform[.]'" *Id.* at *3 n.3 (alteration in original) (quoting the government's filing). "We assume this reasonable conclusion to be true, and thus reasonably conclude that likely hundreds of cellphones other than the suspect's cellphone would be included in the requested geofences." *Id.*

42. See *Global Requests for User Information*, GOOGLE, <https://perma.cc/2YTD-ZMEV> (archived Oct. 23, 2021); Ng, *supra* note 4; *supra* note 11.

43. Valentino-DeVries, *supra* note 3.

compliance with a search warrant.⁴⁴ Tallies have continued to grow, however, and Google received an average of more than thirty geofence warrants per day in 2020.⁴⁵

Police have not limited the use of the SensorVault to egregious or violent crimes.⁴⁶ According to an early geofence-warrant exposé by Minnesota Public Radio, police obtained geofence warrants for an investigation into who had stolen a pickup truck and, separately, \$650 worth of tires.⁴⁷ Separately, Minneapolis investigators used a geofence warrant to identify individuals near an AutoZone where a man had smashed windows during protests over the murder of George Floyd.⁴⁸

It remains unclear if a user can choose to withhold all of her location history from Google, which has asserted that LH sharing is optional for its users.⁴⁹ But manually deactivating all LH sharing remains difficult and discouraged.⁵⁰ A consumer-fraud lawsuit brought by Arizona’s Attorney General alleged that while “Google told users [that] . . . [w]ith Location History off, the places you go are no longer stored,” Google “would surreptitiously collect location information through other settings such as Web & App Activity and use that information to sell ads.”⁵¹ The Associated Press “found that many Google services on Android devices and iPhones store your location data even if you’ve used a privacy setting that says it will prevent Google from

44. See Gabriel J.X. Dance & Jennifer Valentino-DeVries, *Have a Search Warrant for Data? Google Wants You to Pay*, N.Y. TIMES (Jan. 24, 2020), <https://perma.cc/NZP5-5924>.

45. See *supra* notes 11-18 and accompanying text.

46. Magistrate Judge M. David Weisman has lamented the government’s “undisciplined . . . overuse” of geofence warrants in “run-of-the-mill cases that present no urgency or imminent danger.” *In re the Search*, 2020 WL 5491763, at *8.

47. Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MPR NEWS (Feb. 8, 2019, 1:10 PM), <https://perma.cc/HF3G-BP2V>.

48. Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protestors*, TECHCRUNCH (Feb. 6, 2021, 8:00 AM PST), <https://perma.cc/Y6BX-GHLL>.

49. Google Amicus Brief, *supra* note 13, at 5. (“Holders of Google accounts can control various account-level and service-level settings and preferences. ‘Location History’ . . . is an optional account-level Google service. It does not function automatically for Google users.”); *Manage Your Location History*, GOOGLE ACCT. HELP, <https://perma.cc/GP93-XARG> (archived Oct. 23, 2021) (“Location History is turned off by default for your Google Account and can only be turned on if you opt in.”).

50. See Barbara Krasnoff, *Android 101: How to Stop Location Tracking*, VERGE (Aug. 25, 2020, 3:04 PM EDT), <https://perma.cc/X6EQ-5XQ5> (describing the difficult process to deactivate Google location history); Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018), <https://perma.cc/CB84-X5KE> (same).

51. Complaint for Injunctive and Other Relief ¶ 8, *State ex rel. Brnovich v. Google LLC*, No. CV2020-006219 (Ariz. Super. Ct. May 27, 2020) (quoting Nakashima, *supra* note 50).

doing so,” and researchers at Princeton University confirmed these findings.⁵² In 2018, an internal Google email explained that “[t]he current [user interface] feels like it is designed to make [limiting LH collection] possible, yet [it is] difficult enough that people won’t figure it out.”⁵³ Another internal email in 2019 expressed similar frustration: “Speaking as a user . . . I *thought* I had location tracking turned off on my phone. However the location toggle in the quick settings was on.”⁵⁴ The email’s author continued: “[O]ur messaging around this is enough to confuse a privacy focused [software engineer]. That’s not good.”⁵⁵ As one Google employee wrote, “I’d want to know which of these [location-sharing] options (some? all? none?) enter me into the wrongful-arrest lottery.”⁵⁶

And the wrongful-arrest lottery has already begun. In 2018, Arizona police officers jailed Jorge Molina for six days on suspicion of murder.⁵⁷ Officers told Molina that they knew “one hundred percent, without a doubt” that his phone was at the scene of the crime based on a Google geofence warrant.⁵⁸ In reality, Molina had lent an old phone, inadvertently still signed into his Google account, to the man police later arrested for the murder.⁵⁹ In addition to the six days he spent behind bars, Molina lost his job, and “[w]hen he started looking for a new job, he couldn’t get an interview or pass a background check, since a quick Google search showed he had been accused of murder.”⁶⁰ The state impounded Molina’s car during the investigation; eventually, without any income to support himself, Molina lost title to the vehicle.⁶¹

In another nightmarish scenario, Florida police using a geofence warrant to investigate a burglary turned to Google to obtain “more information” on

52. Nakashima, *supra* note 50; *see also* Mark Brnovich (@GeneralBrnovich), TWITTER (May 27, 2020, 3:29 PM), <https://perma.cc/9WYV-QSMB> (“We began our investigation of Google following a 2018 @AP article that detailed how users are lulled into a false sense of security, believing Google provides users the ability to actually disable their Location History.”).

53. Exhibit 18 at 6, State *ex rel.* Brnovich v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. Aug. 21, 2020).

54. Exhibit 215 at 6, State *ex rel.* Brnovich v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. Aug. 21, 2020).

55. *Id.*

56. *Id.* at 4-5.

57. Fussell, *supra* note 6; *see also* Meg O’Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020, 9:11 AM), <https://perma.cc/63PT-K2JM>.

58. Fussell, *supra* note 6 (quoting the police report).

59. *See id.*

60. O’Connor, *supra* note 57.

61. *Id.*

Zachary McCoy.⁶² Google's legal investigations support team notified McCoy that Google would release his data absent court intervention.⁶³ With the help of an attorney, McCoy realized that he was swept into the geofence because, on the day of the burglary, he biked past "the victim's house three times within an hour, part of his frequent loops through his neighborhood."⁶⁴ An avid biker, McCoy used an application called Runkeeper to record his bike rides; Runkeeper "relied on his phone's location services, which fed his movements to Google."⁶⁵ After police withdrew the warrant, McCoy speculated that his entanglement may have ended differently "if his parents hadn't given him several thousand dollars to hire [a lawyer]."⁶⁶

These are but two egregious cases highlighted by news outlets. With hundreds of new geofence warrants filed each week, many similar cases presumably lie unreported.⁶⁷ We now turn to what makes the entanglement of innocents possible by examining the breadth of geofence warrants' reach and the typical geofence-warrant execution process.

B. Warrant Execution

Google has crafted a three-step warrant execution process to handle geofence requests.⁶⁸ As a Google employee stated in a court declaration, "[e]arly 'geofence' legal requests sought LH data that would identify all Google users who were in a geographical area in a given time frame"—essentially an unmasked data dump.⁶⁹ To "ensure privacy protections for Google users and to protect against overbroad disclosures . . . Google instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures."⁷⁰ This has led to the now "typical[]" three-step protocol.⁷¹

62. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, 3:22 AM PST), <https://perma.cc/84NC-K8QQ>.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. Captain John Sherwin of the Rochester Police Department in Minnesota put it colorfully, telling reporters: "When you sit down and think about it, it makes you want to destroy all your devices" and "move to a cabin in Montana." Thomas Brewster, *Feds Order Google to Hand Over a Load of Innocent Americans' Locations*, FORBES (Oct. 23, 2018, 9:00 AM EDT) (quoting Sherwin), <https://perma.cc/5QSU-Y74P>.

68. Declaration of Sarah Rodriguez, *supra* note 10, ¶ 5.

69. *Id.*

70. *Id.*

71. *See id.* ¶¶ 5-12.

1. Initial data dump

In the initial data dump, law enforcement requests from Google the location information of all devices within a specified geographic zone during a defined time frame. The following Figure illustrates one such request.

Figure 1

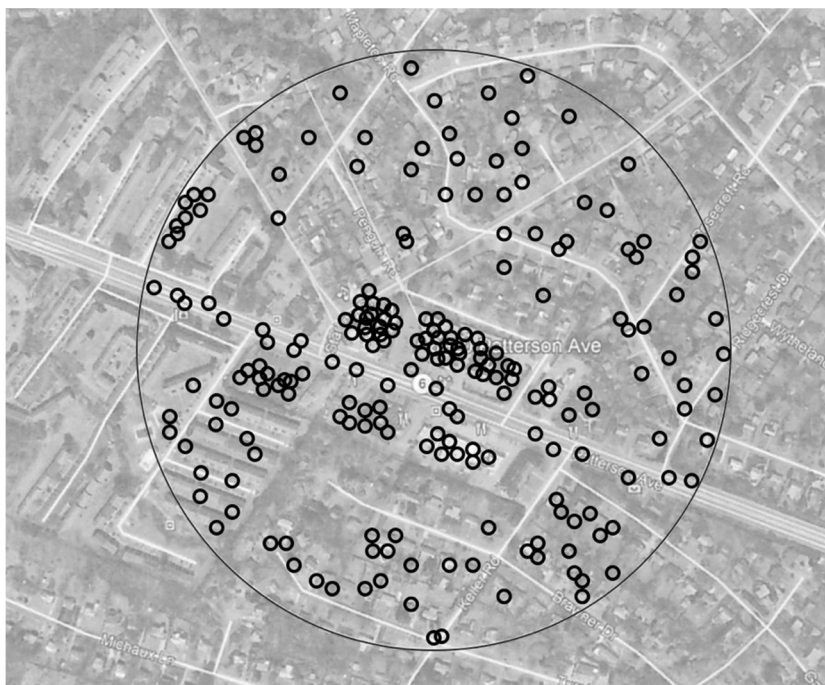


This was one of the geofences requested as part of a Dollar Tree robbery investigation by the FBI in Henrico, Virginia. A significant number of residences and commercial businesses other than the targeted Dollar Tree were within the geofence's geographic zone.

Source: Brewster, *supra* note 67.

In response, Google discloses an anonymized list of devices, each with a unique device ID, timestamps and coordinates, and the data source.⁷²

Figure 2



We created this visual aid to represent what the initial data dump may have looked like to law enforcement, with each circle representing a location ping from a device caught within the boundaries of the geofence.

72. See Brewster, *supra* note 7. Notably, users' supposedly anonymous IDs may not actually be anonymous. A recent exposé on mobile advertising identifiers revealed that these identifiers can be used to piece together personal information about even "masked" users. Charlie Warzel & Stuart A. Thompson, Opinion, *They Stormed the Capitol. Their Apps Tracked Them.*, N.Y. TIMES (Feb. 5, 2021), <https://perma.cc/2J5T-VUHL> (to locate, select "View the live page"). It is not clear whether Google uses mobile advertising identifiers in its data returns.

Figure 3

Device ID	Date	Time (America/Chicago -05:00)	Latitude	Longitude	Source	Maps Display Radius (m)
-1025956090	4/8/2019	11:07:00 (-05:00)	43.4214456	-88.3507382	GPS	9
-1361086191	4/8/2019	10:52:33 (-05:00)	43.4211171	-88.3508743	GPS	16
-1638700124	4/8/2019	10:54:57 (-05:00)	43.421202	-88.3503325	WiFi	58
1565184502	4/8/2019	10:55:12 (-05:00)	43.4313883	-88.35045	GPS	3
1830501424	4/8/2019	11:05:24 (-05:00)	43.4211382	-88.3500203	WiFi	50
647939400	4/8/2019	10:56:03 (-05:00)	43.421015	-88.350123	WiFi	59

This is what the initial data dump looks like on paper. This particular list was the location history returned to law-enforcement officials investigating a bank robbery in Allenton, Wisconsin.

Source: Brewster, *supra* note 7.

The precision of the latitude and longitude coordinates varies depending on source, as demonstrated by Figure 3’s rightmost column, “Maps Display Radius (m).”⁷³ For GPS-derived latitude and longitude coordinates, Google provides maps display radii (i.e., certainty of a user’s location) ranging from three to sixteen meters. For coordinates derived via Wi-Fi, however, Google provides radii ranging from fifty to fifty-nine meters. As shown in Figure 3, Google was able to approximate the coordinates derived using GPS more precisely than those derived via Wi-Fi. As a Google product manager noted, “[I]f a user opens Google Maps and looks at the blue dot indicating Google’s estimate of his or her location, Google’s goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.”⁷⁴

73. This is the circle that a user sees when they open up a map-based application on their mobile device: The larger the radius of the circle, the less precise the reported location of the user. See *Find & Improve Your Location’s Accuracy*, GOOGLE MAPS HELP, <https://perma.cc/C4MC-QXR7> (archived Jan. 28, 2022); Ellis, *supra* note 24. See generally Krista Merry & Pete Bettinger, *Smartphone GPS Accuracy Study in an Urban Environment*, 14 PLOS ONE, no. 7, July 2019, at 1, 2-3, 17 (noting that the accuracy of a smartphone’s reported location data can vary widely depending on a number of variables).

74. Declaration of Marlo McGriff, *supra* note 9, ¶ 24. Geofence warrants do not necessarily limit the data searched to the subset of users actually present in the geofence. Depending on how a corporation indexes data, all accounts may need to be queried to identify records that match the warrant’s specified place and time. This is the case for Google, which has stated that its database is structured such that it requires a search of all users to produce the initial data dump. See Google Amicus Brief, *supra* note 13, at 12-13.

Accordingly, law enforcement may obtain data for users outside of the warrant’s geographic parameters who, due to imprecision, logged a location radius that fell within the geofence.⁷⁵ The following example illustrates such a possibility. Focusing on two devices in our geofence, Device 1 and Device 2, let us assume (1) that Device 1 has location coordinates derived from Wi-Fi with a radius of fifty-five meters; and (2) that Device 2 has location coordinates derived from a cell site with a radius of 1,000 meters (a radius that can be typical for locations based on cell sites⁷⁶).

The radius of Device 1 would look like this:

Figure 4

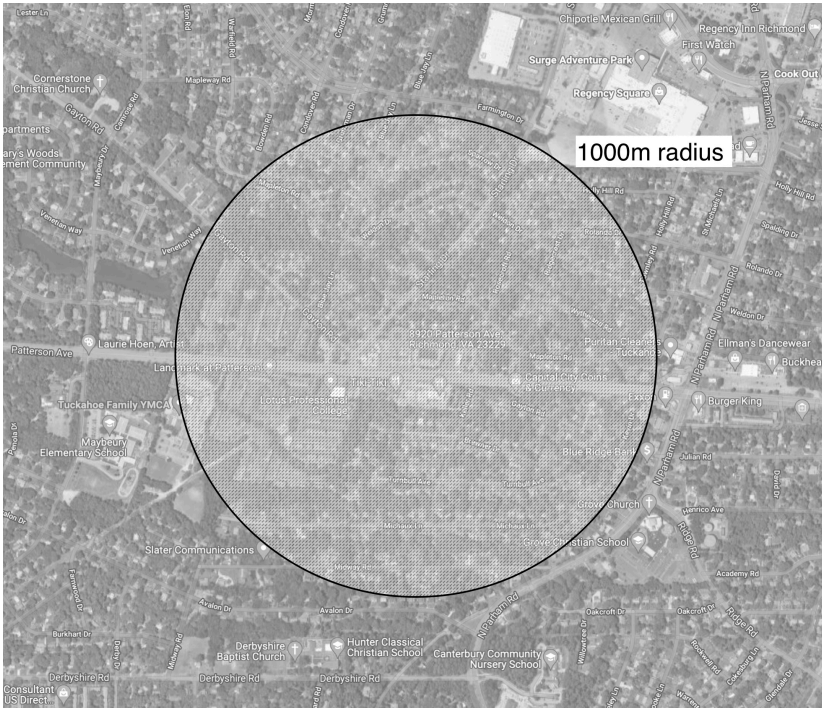


75. See Declaration of Marlo McGriff, *supra* note 9, ¶ 25.

76. Ellis, *supra* note 24.

The radius of Device 2 would look like this:

Figure 5



Therefore, as illustrated in particular for Device 2 (because of its large radius), it is possible that an individual can end up in a geofence for an area in which they were never present. This issue may not be a concern for targeted advertisements: Accidentally serving ads to people outside of the intended geographic area carries little harm beyond wasted effort and money.⁷⁷ But the same flaw in precision carries far more serious consequences when the SensorVault is used for criminal liability.

77. Indeed, a Google product manager explained that Google's ability to approximate device location "is sufficiently precise and reliable for [the] purposes for which Google designed LH." Declaration of Marlo McGriff, *supra* note 9, ¶ 26.

2. Selective expansion

After law-enforcement officials review the data in the initial dump, the next step is selective expansion. Without the oversight of a magistrate judge, law enforcement requests additional location history for certain devices in the geofence.⁷⁸ The expanded location history reaches beyond the geographic and temporal ranges specified in the initial data dump, enabling law enforcement to track the path of devices before and after the window in which the crime allegedly occurred.⁷⁹ This information can lead officials to discard some devices from the investigation and focus more deeply on others (if, for example, a device's trajectory aligns with the known escape route of an unidentified person of interest).⁸⁰

The original warrant typically governs the time frame beyond the original window for which law enforcement can request geographically unbounded LH. For example, one geofence warrant told Google to "provide additional location history outside of the predefined area for . . . relevant accounts to determine path of travel" for up to forty-five minutes before or after the originally enumerated time windows.⁸¹ Another geofence warrant permitted investigators to request additional data from "30 minutes before AND 30 minutes after the initial search time periods."⁸²

78. See, e.g., Defendant Okello Chatrie's Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 6, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Oct. 29, 2019), 2019 WL 7660969, ECF No. 29 [hereinafter *Chatrie Motion to Suppress*]; see also Valentino-DeVries, *supra* note 3.

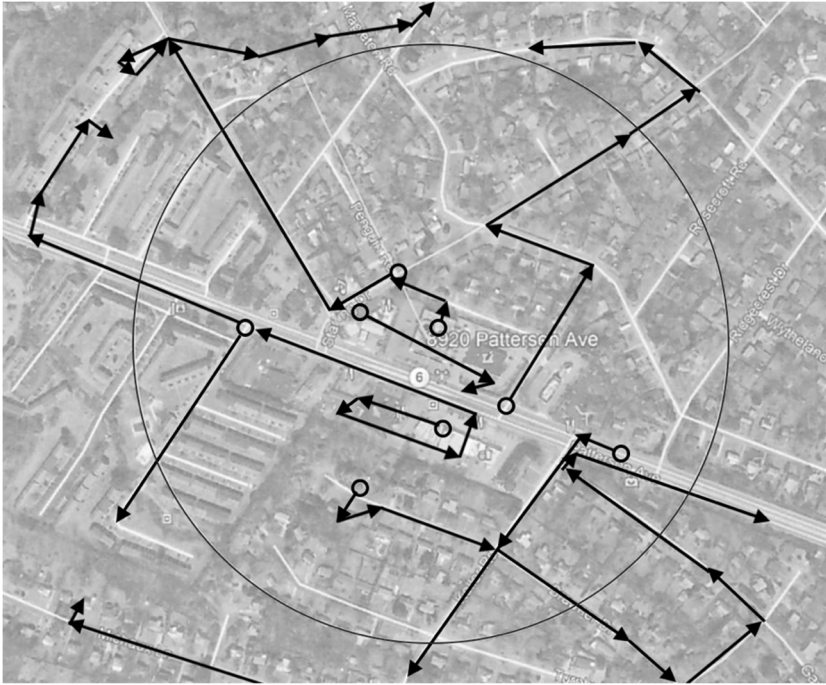
79. See, e.g., *Chatrie Motion to Suppress*, *supra* note 78, at 6 (describing how investigators, without judicial scrutiny, gained access to the unbounded location data of nine users for thirty minutes before and after the initial geofence time period).

80. The selective-expansion step is sometimes omitted for geofence warrants that examine multiple time frames. See, e.g., Application for a Search Warrant at 16-17, *In re the Search of: Location & Identifying Info.* Maintained by Google LLC, No. 19-mj-00918 (E.D. Wis. Dec. 31, 2019), ECF No. 1 [hereinafter Dec. 31, 2019 Application]; Application for a Search Warrant at 20-22, *In re the Search of: Location Hist. Data from Google LLC Generated from Mobile Devices*, No. 19-mj-00104 (E.D. Wis. Dec. 4, 2019), ECF No. 1; Application for a Search Warrant at 14-16, 19, *In re the Search of: Location Hist. Data from Google LLC Generated from Mobile Devices*, No. 19-mj-00846 (E.D. Wis. May 1, 2019), ECF No. 1; Application for a Search Warrant at 9, 11, 13-14, *In re the Search of: Info. That Is Stored at Premises Controlled by Google*, No. 18-mj-01307 (E.D. Wis. Nov. 20, 2018), ECF No. 1. This may be because investigators are able to identify devices of interest based on multiple appearances.

81. Motion to Quash & Suppress Evidence Under Penal Code §§ 1538.5 & 1546 at 8, *People v. Dawes*, No. 19002022 (Cal. Super. Ct. June 9, 2020) [hereinafter *Dawes Motion to Quash & Suppress*] (emphasis omitted) (quoting the warrant).

82. *Chatrie Motion to Suppress*, *supra* note 78, at 6 (quoting the warrant).

Figure 6



A visual representation of the selective-expansion step, showing location history outside of the originally specified time and radius for devices identified for additional data production.

3. Unmasking

Lastly, and again without judicial oversight, law enforcement requires Google to provide subscriber information for any device selected by investigators.⁸³ This unmasking divulges information including the account's registered name, address, start date of service, services utilized, telephone

83. See, e.g., *Chatrre Motion to Suppress*, *supra* note 78, at 6-7; see also Valentino-DeVries, *supra* note 3. Note that Minnesota police officers follow a different practice: After they receive the initial data dump, they request another warrant from the court to retrieve identifying information. Aaron Mak, *Close Enough*, SLATE (Feb. 19, 2019, 5:55 AM), <https://perma.cc/72YG-393W>.

numbers, email addresses, and means and sources of payment for services.⁸⁴ In at least one instance, law enforcement has sought personal identifying information from all devices included in the initial data dump.⁸⁵

II. Geofences and the Fourth Amendment

Geofence warrants raise a series of Fourth Amendment questions, some more explored than others in the context of new technologies.

A. Is a Geofence a Fourth Amendment “Search”?

The threshold question is, of course, whether a geofence is a search—that is, whether it invades a “reasonable expectation of privacy” per the test formulated by Justice Harlan’s concurrence in *Katz v. United States*.⁸⁶ In perhaps the most relevant precedent addressing law enforcement’s investigatory use of consumer data, *Carpenter v. United States*, the Court grappled with this question in the context of cell-site location information used to catalog a suspect’s whereabouts over the course of several days.⁸⁷ Rejecting an application of the third-party doctrine (given that the data was in the possession of the suspect’s cell-service provider),⁸⁸ the Court held that the government’s acquisition of this data was a search and that the government should have obtained a probable-cause warrant in order to access it.⁸⁹ However, the Court ended its opinion with a caveat, explaining that the decision was narrow and cabined to its facts.⁹⁰

The *Carpenter* caveat opened the door to a cottage industry of litigation over whether, under *Carpenter*’s reasoning, the use of other technologies can also amount to a Fourth Amendment search.⁹¹ One prominent unanswered question in this inquiry is whether the government can avoid *Carpenter*’s warrant requirement by using many small intrusions over a large population

84. See, e.g., Dec. 31, 2019 Application, *supra* note 80, at 17; cf. 18 U.S.C. § 2703(c)(2) (describing the required disclosures in response to a Stored Communications Act subpoena for subscriber information).

85. Brewster, *supra* note 7.

86. See 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

87. 138 S. Ct. 2206, 2212–13, 2216–17 (2018).

88. Traditionally, under the third-party doctrine, “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

89. *Carpenter*, 138 S. Ct. at 2221, 2223.

90. *Id.* at 2220.

91. See *supra* note 27.

(as it does with geofence warrants) rather than a few large intrusions over a small population (as it did in *Carpenter*).⁹²

In addition to its unclear scope, *Carpenter*'s longevity is uncertain. The recent change in Supreme Court membership (with the passing of Justice Ginsburg and the confirmation of Justice Barrett) means that the five-vote *Carpenter* majority is no longer intact. Attention has now turned to Justice Gorsuch's *Carpenter* dissent as a possible path forward.⁹³ Justice Gorsuch's theory employs a positive-law approach, suggesting that a user may retain a property interest in his or her data held by a third-party provider.⁹⁴

Accordingly, an in-depth analysis of the *Carpenter* question—whether a geofence warrant constitutes a Fourth Amendment search—is not the main focus of this Note. Google's policy of objecting to anything less than a probable-cause warrant has seemingly pressured the government to file only warrant applications, punting the resolution of the *Carpenter* question further down the line.⁹⁵ And at least one court to consider the *Carpenter* question in the geofence context has noted that *Carpenter* is not dispositive. In a 2020 opinion denying a geofence warrant, Magistrate Judge M. David Weisman wrote that a citation to *Carpenter* was "not intended to suggest that *Carpenter* pre-ordains the outcome here."⁹⁶ Instead, Judge Weisman's opinion was "premised on much longer established Fourth Amendment principles that a search warrant must establish probable cause to justify the scope of the search requested, and the type of evidence to be seized must be particularly described, not left to the agents' complete discretion."⁹⁷ The court thus found that the only dispositive question was whether the geofence warrant could be properly issued under the magistrate's authority, bound to the probable-cause and particularity issues we discuss in Parts IV and V below.

92. This question raises a related issue: If there is a search, when does the search occur? Is it at the time Google queries the database, or is it when law enforcement gains access to the data? See generally Note, *supra* note 24, at 2515-20 (arguing that a search occurs "when a private company first searches through its entire database"). For the purposes of this Note, the distinction makes no difference. Even if the search occurs when data is returned to law enforcement, the search still cannot satisfy probable-cause and particularity requirements. See *infra* Part IV.

93. See, e.g., Chris Machold, Note, *Could Justice Gorsuch's Libertarian Fourth Amendment Be the Future of Digital Privacy? A "Moderate" Contracts Approach to Protecting Defendants After Carpenter*, 53 U.C. DAVIS L. REV. 1643, 1648-49 (2020) (noting that Justice Gorsuch's *Carpenter* dissent offers a promising path to a majority that can protect the digital privacy interests of defendants).

94. See *Carpenter*, 138 S. Ct. at 2267-72 (Gorsuch, J., dissenting).

95. See *infra* Parts III.A-C.

96. *In re the Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-00297, 2020 WL 5491763, at *7 n.10 (N.D. Ill. July 8, 2020).

97. *Id.*

But to briefly indicate our intuitions on the *Carpenter* question: We agree with the court decisions and commentators arguing that *Carpenter*'s holding extends beyond its factual boundaries.⁹⁸ And we believe that *Carpenter* extends to geofence technology. Whether a geofence request is viewed as a search of many individuals, a search of many individual devices, or a search of many homes, a geofence violates the reasonable expectation of privacy of each user swept up in its bounds. It is near axiomatic to say that users today have, or should have, a reasonable expectation of privacy in their sensitive location data. Location data is qualitatively different than other kinds of data: It is precise and revealing,⁹⁹ and it is in many ways the currency of the modern era. Some companies compete by limiting third-party access to location data; others use dubious means to mine it.¹⁰⁰ And cell-site location information—the kind of data that the *Carpenter* Court found precise enough to warrant Fourth Amendment protection—is the least precise form of location input.¹⁰¹

Any argument that a geofence search is less privacy invasive because it gathers data only in a short time window is misguided. Mere minutes of the SensorVault's pinpointed LH can be incredibly revealing.¹⁰² In fact, this is often the precise reason that law-enforcement officials seek LH: As a Minnesota deputy police chief admitted, SensorVault's constant, precise tracking "shows the whole pattern of life," a "game changer for law enforcement."¹⁰³ And even a brief snapshot can expose highly sensitive information—think a visit to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar,"¹⁰⁴ or a location other than home during a COVID-19 shelter-in-place order.

98. See, e.g., *State v. Sylvestre*, 254 So. 3d 986, 991-92 (Fla. Dist. Ct. App. 2018) (holding that *Carpenter* extends to cell-site simulator location data); Freiwald & Smith, *supra* note 27, at 227-31.

99. See *Carpenter*, 138 S. Ct. at 2212 (noting that "modern cell phones generate increasingly vast amounts of increasingly precise" cell-site location information).

100. See, e.g., Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolick, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), <https://perma.cc/R8QW-XWCF> (to locate, select "View the live page"); Chaim Gartenberg, *Why Apple's New Privacy Feature Is Such a Big Deal*, VERGE (Apr. 27, 2021, 10:30 AM EDT), <https://perma.cc/H8LT-24GC>; Brian X. Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice*, N.Y. TIMES (updated Sept. 29, 2021), <https://perma.cc/PJN5-RB6N>.

101. *Carpenter*, 138 S. Ct. at 2220; Ellis, *supra* note 24.

102. See *supra* Part I.A.

103. Valentino-DeVries, *supra* note 3 (quoting Brooklyn Park Deputy Police Chief Mark Bruley).

104. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

There are also real doubts as to whether anonymization actually protects the privacy of users whose data is revealed in a geofence. As researchers have repeatedly proven, cross-referencing datasets can reveal the identifying information of nearly every “anonymized” user.¹⁰⁵ There are many opportunities to cross-reference an anonymized data dump received from Google, invading the privacy of all users caught up in the geofence.

Regarding an application of the third-party doctrine, there is real doubt as to whether users voluntarily share their location data with Google.¹⁰⁶ As detailed above, even sophisticated Google employees struggle to understand how, if at all, they can turn off LH collection.¹⁰⁷ And even if it is theoretically possible to stop Google’s location tracking, the briefing for *United States v. Chatrie* has documented the lack of voluntariness of the initial consent:

Following the standard setup of an Android phone like the one used by Mr. Chatrie, a user encounters a pop-up screen . . . when opening the Google Maps application for the first time. It says, “Get the most from Google Maps” and then it gives the user two options: “YES I’M IN” or “SKIP.” There is also a statement that reads “Google needs to periodically store your location to improve route recommendations, search suggestions, and more” and a button to “LEARN MORE.” The pop-up does not use the phrase [sic] “Location History,” but clicking on “YES I’M IN” enables the function. Clicking on “LEARN MORE” takes the user to a webpage with Google’s complete Privacy Policy and Terms of Service; it does not direct the user to any specific language concerning location data or Location History specifically.

In fact, Google’s Terms of Service do not mention Location History at all. And Google’s Privacy Policy, which is 27 pages long, mentions Location History only twice. In the first instance, it says, in full: “You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.” If anything, the phrase “private map” is misleading and suggests that Google does not have access to the data. In the second instance, the policy says, in full: “Decide what types of activity you’d like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.” Of course, “traffic predictions” do not begin to suggest that Google will keep a 24/7 “journal” of a user’s whereabouts. But even if it did, a user would have no way of knowing that the pop-up “opt-in” screen relates to the Location History feature.

105. The inability of users to stop sharing location data with cell-service providers helped motivate the holding in *Carpenter*. See *Carpenter*, 138 S. Ct. at 2220 (“[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.”).

106. Warzel & Thompson, *supra* note 72; Gina Kolata, *Your Data Were “Anonymized”? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), <https://perma.cc/73J2-PXUQ>.

107. See *supra* notes 53-56 and accompanying text.

The pop-up does not reference “Location History” by name. As a result, a typical user would not know to scour Google’s policies for references to Location History, much less understand the implications of the choice Google is asking them to make. In short, it is strikingly easy for a user to “opt-in” to Location History without ever being aware of doing so.¹⁰⁸

Another *Chatrie* defense brief details the similarly confusing maze a user must navigate to pause and delete LH data.¹⁰⁹

Even if the Supreme Court adopts Justice Gorsuch’s theory that a provider may serve as a bailee of data,¹¹⁰ we believe that the Fourth Amendment still applies to geofence searches. Users likely have a property interest in their SensorVault information, and those individuals who knowingly opt into LH collection affirmatively designate Google as a bailee.

B. Probable Cause, Particularity, and Warrant Execution

Because of Google’s policies and the uncertainty surrounding *Carpenter*,¹¹¹ geofence issues have primarily been situated in less explored Fourth Amendment questions: (1) when a search warrant is properly issued per the requirements of probable cause and particularity; and (2) how a warrant is properly executed. A brief primer on the relevant case law: A valid search warrant can only issue upon a showing of probable cause to the issuing neutral magistrate.¹¹² In rare circumstances—primarily in administrative or regulatory searches, where a public need and the lack of an ordinary criminal investigation justify an intrusion—investigative techniques are subjected to a relaxed probable-cause requirement.¹¹³

The Fourth Amendment also instructs that no warrants shall issue except those “particularly describing the place to be searched, and the persons or things to be seized.”¹¹⁴ The Supreme Court has explained that this requirement “makes general searches under [warrants] impossible and prevents the seizure

108. Defendant Okello Chatrie’s Supplemental Motion to Suppress Evidence Obtained from a “Geofence” General Warrant at 15-17, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. May 22, 2020), 2020 WL 4551093, ECF No. 104 [hereinafter *Chatrie* Supplemental Motion to Suppress] (footnotes omitted) (citations omitted).

109. *Chatrie* Post-hearing Brief, *supra* note 20, at 14-15.

110. *See Carpenter*, 138 S. Ct. at 2268-69 (Gorsuch, J., dissenting); *supra* notes 93-94 and accompanying text.

111. *See supra* notes 92-97 and accompanying text.

112. *See* U.S. CONST. amend. IV; *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971), *overruled in part on other grounds by Horton v. California*, 496 U.S. 128 (1990); *Johnson v. United States*, 333 U.S. 10, 13-15 (1948).

113. *See infra* Part IV.A.3.

114. U.S. CONST. amend. IV.

of one thing under a warrant describing another.”¹¹⁵ The particularity requirement also limits the discretion of an officer executing a warrant and “determines the permissible intensity” and scope of the search.¹¹⁶ For example, a search warrant describing an entire apartment building will usually be held invalid without a probable-cause showing as to all the units in the building.¹¹⁷ Similarly, a warrant authorizing the search of a specified area and “any and all persons found therein” is likely defective if it does not establish that (1) someone present during the warrant execution is likely involved in the criminal activity; and (2) the individual likely has evidence of the crime on his or her person.¹¹⁸ And once the original warrant is executed, the place cannot be searched a second time unless a second warrant is obtained from the court, coupled with an affidavit detailing why there is probable cause to search again notwithstanding the first warrant.¹¹⁹

III. How Courts Are Handling Geofence Warrants

Amid a lack of binding state and federal jurisprudence, magistrate judges in the U.S. District Court for the Northern District of Illinois and the U.S. District Court for the District of Kansas have collectively produced five opinions on geofence warrants. Three of the Illinois opinions reject geofence-warrant applications but leave open the possibility of a constitutionally permissible geofence request. Similarly, the Kansas opinion rejects a geofence-warrant application based on its lack of probable cause and particularity without categorically ruling geofence warrants unconstitutional. The fourth Illinois opinion approves a geofence-warrant application.

The first geofence-warrant challenge before an Article III federal judge is underway in *United States v. Chatrie*, with the issue briefed and argument pending at the time of writing.¹²⁰ Similarly, a state court opinion examining

115. *Marron v. United States*, 275 U.S. 192, 196 (1927).

116. 2 WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, *CRIMINAL PROCEDURE* § 3.4(f) (West 2021).

117. *Id.* § 3.4(e).

118. *Id.* (collecting cases).

119. *Id.* § 3.4(j); see *United States v. Baldyga*, 233 F.3d 674, 682-83 (1st Cir. 2000).

120. See Defendant’s Response to the Government’s Supplemental Memorandum in Opposition to Defendant’s Discovery of SensorVault Data at 12, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Feb. 25, 2020), ECF No. 92 (“The Court has recognized that this is ‘a case of first impression . . .’” (quoting Complete Transcript of Discovery Motion Before the Honorable M. Hannah Lauck at 179, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Jan. 30, 2020), ECF No. 81)); Andrea Vittorio, *Robbery Poses Legal Test for Police Use of Google Location Data*, BLOOMBERG L. (Sept. 14, 2021, 2:01 AM), <https://perma.cc/Z38W-F8YB> (noting that *Chatrie* “is considered the first federal example of a criminal defendant challenging the use of a [geofence] data as

footnote continued on next page

the constitutionality of geofence warrants could emerge from a challenge currently underway in California's San Francisco County Superior Court in *People v. Dawes*.¹²¹

This Part walks through the Northern District of Illinois and District of Kansas cases and examines both *Chatrie* and *Dawes*. It then concludes with preliminary takeaways from the nascent geofence litigation.

A. Northern District of Illinois Magistrate Opinions

Northern District of Illinois magistrate judges have taken the lead in considering the constitutional questions surrounding geofence warrants. They have done so in four opinions across two investigations. In the first investigation, regarding the theft and sale of pharmaceuticals, law enforcement requested a geofence warrant three separate times.¹²² Magistrate judges denied all three requests.¹²³

A second investigation, regarding a series of arsons, involved one geofence-warrant request and yielded an unsealed opinion granting the warrant.¹²⁴ This opinion, while far from the first grant of a geofence warrant, represents the first published opinion approving a geofence warrant and asserting the warrant's constitutionality.¹²⁵

In the first investigation, the government sought a geofence warrant to investigate "the theft and resale of certain pharmaceuticals."¹²⁶ The government requested three specific geofences, all for forty-five-minute periods, across three different days.¹²⁷ The first covered a 100-meter radius

evidence in his indictment"); Sobel, *supra* note 24 (identifying *Chatrie* as "the first known federal Fourth Amendment challenge against a geofence warrant in a federal district court").

121. See *Dawes* Motion to Quash & Suppress, *supra* note 81, at 1-2. One of the authors of this Note was an author of the motion to quash and suppress in *Dawes*.

122. *In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 732-33 (N.D. Ill. 2020).

123. *Id.* at 732-33, 757; see also Sealed Memorandum Opinion & Order at 1, 25, *In re the Search of: Info. Stored at Premises Controlled by Google*, as Further Described in Attachment A, No. 20-mc-00392 (N.D. Ill. July 24, 2020), ECF No. 5; *In re the Search of: Info. Stored at Premises Controlled by Google*, as Further Described in Attachment A, No. 20-mc-00297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020), ECF No. 4.

124. *In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 349, 351 (N.D. Ill. 2020).

125. See *In re the Search*, 481 F. Supp. 3d at 748 ("The Court is not aware of any federal decision addressing [probable-cause and particularity] issues with respect to a geofence warrant, and the Court has reason to believe that geofence warrants are facing their first round of judicial scrutiny.").

126. *In re the Search*, 2020 WL 5491763, at *1.

127. *Id.*

(over 7.7 acres of land) during the afternoon in “a densely populated” area containing “restaurants, various commercial establishments, and at least one large residential complex.”¹²⁸ The second and third, both of which also covered 100-meter radii during the afternoon, included “medical offices and other single and multi-floor commercial establishments that are likely to have multiple patrons.”¹²⁹

1. Pharmaceutical sale investigation: first denial

The first warrant application requested only the initial data dump and unmasking steps.¹³⁰ Magistrate Judge M. David Weisman’s opinion roundly rejected the government’s application. Judge Weisman indicated his “only point of agreement” with the government’s argument was probable cause for the suspect: “There is probable cause to believe that among all the other data this warrant application seeks from Google, there is a likelihood that the suspect’s phone data would be included.”¹³¹ But the warrant, he wrote, “suffers from two obvious constitutional infirmities.”¹³² “First, the scope of the search is overbroad, and second, the items to be seized are not particularly described.”¹³³

Judge Weisman explained that it “strains credibility” in a probable-cause inquiry to assert that individuals within the entire geofence bore witness to the illegal pharmaceutical transaction, which involved receipt indoors of a mailed package.¹³⁴ Witnessing such an act, he colorfully speculated, would have required the individuals to “possess extremely keen eyesight and perhaps x-ray vision to see through . . . many walls.”¹³⁵ Judge Weisman also noted that “the majority of the area sought encompasses structures and businesses that would necessarily have cell phone users who are not involved in [the underlying] offenses.”¹³⁶

In explaining why the government’s request was not narrowly tailored, the opinion noted that “the geographic scope of this request [is] a congested urban area encompassing individuals’ residences, businesses, and healthcare providers,” meaning that the “vast majority of cellular telephones likely to be

128. *Id.* at *1, *3.

129. *Id.* at *1.

130. *See id.*; *supra* Part I.B.

131. *In re the Search*, 2020 WL 5491763, at *4.

132. *Id.* at *3.

133. *Id.*

134. *Id.* at *5 & n.6.

135. *Id.*

136. *Id.* at *3.

identified in this geofence will have nothing whatsoever to do with the offenses under investigation.”¹³⁷ Judge Weisman rejected the government’s assertion that the warrant’s multistep process would protect people’s privacy, finding that “the warrant does not limit agents to only seeking identifying information as to the ‘five phones located closest to the center point of the geofence,’ or some similar objective measure of particularity.”¹³⁸

2. Pharmaceutical sale investigation: second denial

After the denial by Judge Weisman, the government submitted two additional warrant applications, both of which were denied.

In its second application, the government added a request that the areas to be searched include “the location history for such devices that ‘could have been (as indicated by margin of error, i.e. “maps display radius”) located within’ the geographical area of the geofences . . . within the time and date parameters of the geofences.”¹³⁹ The court explained that the “purpose of including this ‘margin of error’ . . . appears to be directed at ensuring that the proposed warrant captures the location histories for Google-connected devices within the margin of error, i.e., to minimize the possibility that the geofences would miss or overlook a device that may have been inside” the relevant locations.¹⁴⁰ Magistrate Judge Gabriel Fuentes objected to this inclusion, noting that “even a small-scale expansion of the boundaries” of the geofences in question would increase “the chances that the information of uninvolved users would fall within the reach of the government at its discretion.”¹⁴¹

The government’s second application also narrowed the geographic scope of the three proposed geofences, keeping the searches closer to the two physical locations at issue.¹⁴² Judge Fuentes found that the narrowing of the geofence boundaries did not “solve the constitutional problem,” however, because “the Court still has no idea how many . . . devices and their users will be identified under the warrant’s authority.”¹⁴³ In other words, “the information of an undetermined number of uninvolved persons is authorized to be seized.”¹⁴⁴

137. *Id.* at *5 (footnote omitted).

138. *Id.* at *5-6.

139. Sealed Memorandum Opinion & Order, *supra* note 123, at 15 (quoting the application); *see supra* notes 73-75 and accompanying text.

140. Sealed Memorandum Opinion & Order, *supra* note 123, at 16.

141. *Id.* at 16-17.

142. *Id.* at 11-12, 14-15.

143. *Id.* at 22.

144. *Id.* The government also argued that a stay-at-home order reduced the number of innocent people at one of the geofence locations, but the court responded that it “still has no way of knowing how many Google-connected devices traversed the busy urban
footnote continued on next page

3. Pharmaceutical sale investigation: third denial

In the government's third geofence application, the requested geographic and temporal scope remained unchanged from the second application.¹⁴⁵ Although the third application eliminated the unmasking step requested in the initial warrant, the government subsequently clarified that it "retain[ed] the power to obtain by subpoena the identifying subscriber information for any of the device IDs on the anonymized list."¹⁴⁶ The government also "limit[ed] the 'anonymized' information [sought] to that which 'identifies individuals who committed or witnessed the offense,'" yet it provided "[n]o further methodology or protocol" explaining "how Google would know which of the sought-after anonymized information identifies suspects or witnesses."¹⁴⁷

According to Judge Fuentes, elimination of the unmasking step neither altered the analysis nor cured any constitutional infirmity.¹⁴⁸ The government's ability to obtain personal information from Google's list via subpoena, he reasoned, implicated "the principle that the government may not accomplish indirectly what it may not do directly."¹⁴⁹ Judge Fuentes also held that a "too-vague, eight-word caveat that the information is limited to that which 'identifies the individuals who committed or witnessed the [offense]'" could not cure the application's constitutional infirmity.¹⁵⁰ More specific protocols for Google to determine which devices belonged to relevant persons, he wrote, were necessary.¹⁵¹ Judge Fuentes reiterated that the proposed warrant's "harness[ing of] geofence technology to cause the disclosure of the identities of various persons" meant that "the government must satisfy probable cause as to those persons," which it had still failed to do.¹⁵²

area of [that geofence], and to assume the number of persons was reduced by the stay-at-home order based on the statistics the government presented would be pure speculation." *Id.* at 23.

145. *In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 732-33 (N.D. Ill. 2020) (stating that the three forty-five-minute geofences contained in the third application were unchanged in geographic scope from the second application).

146. *Id.* at 733.

147. *Id.* (quoting the application).

148. *Id.* at 749.

149. *Id.*

150. *Id.* at 750 (quoting the application).

151. *See id.*

152. *Id.* at 750-51.

4. Arson investigation

In the second investigation that produced an unsealed federal magistrate's opinion, the government presented a geofence warrant application in connection with "a series of approximately 10 arsons in the Chicago area."¹⁵³ Law enforcement believed that the fires, most of which burned vehicles, were connected, and that the geofences would "contain evidence pertaining to the identity of the arson suspects and their co-conspirators."¹⁵⁴ The government requested six geofences, four located in commercial lots where the vehicle fires had occurred and two along areas of roadway where the unknown arsonists were alleged to have traveled.¹⁵⁵ Each spanned between fifteen and thirty-seven minutes in length during early morning hours.¹⁵⁶ All but one covered less than a city block, with the fourth proposed geofence covering an elongated roadway area "approximately the length of 1.25 city blocks."¹⁵⁷ Similar to the first investigation, the second investigation's warrant application requested a two-step execution: the initial data dump followed by unmasking.¹⁵⁸

Magistrate Judge Sunil Harjani approved the application, explaining that, "[o]nce novel," geofence warrants are "now more frequent in criminal investigations" and finding that the application "satisfies the probable cause and particularity requirements of the Fourth Amendment."¹⁵⁹ Judge Harjani held that there was "probable cause that evidence of the crime will be located at Google because location data on cell phones at the scene of the arson, as well as the surrounding streets, can provide evidence on the identity of the perpetrators and witnesses to the crime."¹⁶⁰ Based on the government's assertions that (1) the alleged arsonists likely "use[d] cell phones to plan and commit criminal offenses"; and (2) "there was a reasonable probability that a cell phone, regardless of its make, is interfacing in some manner with a Google application, service, or platform," the court concluded that "there is a fair probability that location data at Google will contain evidence of the arson crime, namely the identities of perpetrators and witnesses to the crime."¹⁶¹

The court also held that the geofences were sufficiently limited in scope: They were "specific to the time of the arson incidents only" and "narrowly

153. *In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 351 (N.D. Ill. 2020).

154. *Id.*

155. *Id.* at 351-53.

156. *Id.*

157. *Id.*

158. *See id.* at 353; *supra* note 130 and accompanying text.

159. *In re the Search Warrant Application*, 497 F. Supp. 3d at 349.

160. *Id.* at 355.

161. *Id.* at 356.

crafted to ensure that location data, with a fair probability, will capture evidence of the crime only.”¹⁶² The court noted that the warrant request was appropriately narrow because the buildings and streets contained in the geofences were unlikely to be occupied during the early-morning times requested.¹⁶³ The court also explained that a margin of error for location-history data, the “exact scope” of which “is unknown,” did not render the warrant unconstitutional.¹⁶⁴ In the court’s eyes, “the fact that warrants for location data have margins of error does not invalidate them—only reasonableness is required, not surgical precision.”¹⁶⁵ Because the margin of error was “reasonable given the nature of the evidence being sought and what is possible with the technology at issue,” the court found that the warrant met the particularity requirement.¹⁶⁶

B. District of Kansas Magistrate Opinion

In June 2021, Magistrate Judge Angel Mitchell of the U.S. Court for the District of Kansas denied a federal geofence-warrant application on Fourth Amendment grounds.¹⁶⁷ The opinion did not provide much detail regarding the nature of the geofence sought, stating only that the requested data would have covered an area surrounding “a sizeable business establishment” during a one-hour period.¹⁶⁸ Judge Mitchell paid significant attention to the Northern District of Illinois opinions surveyed in Part III.A above.¹⁶⁹ Guided by the analysis in those cases, Judge Mitchell held that the submitted application and affidavit were “not sufficiently specific or narrowly tailored to establish probable cause or particularity.”¹⁷⁰

Judge Mitchell’s opinion emphasized that probable cause relates to both (1) whether a crime has been committed; and (2) whether evidence of the crime will be located at the place to be searched.¹⁷¹ In surveying the evidence, Judge Mitchell concluded there was “probable cause that a crime was committed at

162. *Id.* at 357.

163. *Id.* at 358.

164. *Id.* at 360-61.

165. *Id.* at 361.

166. *Id.*

167. *In re the Search of Info. That Is Stored at the Premises Controlled by Google, LLC*, No. 21-mj-05064, 2021 WL 2401925, at *1 (D. Kan. June 4, 2021).

168. *Id.* at *2; *see also id.* at *4 (noting that the geofence boundary “encompasses two public streets,” that “the subject building contains another business,” and that “the area just outside of the perimeter . . . includes residences and other businesses”).

169. *See id.* at *1-4.

170. *Id.* at *1.

171. *Id.* at *2.

the [geofence location] during the relevant one-hour time period.”¹⁷² She found that the government had failed, however, to “establish probable cause that evidence of the crime will be located at the place searched—that is, Google’s records showing the location data of cell phone users within the geofence boundaries.”¹⁷³ In her judgment, Google’s stored location data “would undoubtedly show” where certain devices were located at a given point in time.¹⁷⁴ But the government’s statements were “too vague and generic to establish a fair probability—or any probability—that the identity of the perpetrator or witnesses would be encompassed within the search.”¹⁷⁵ Even if the court assumed that most individuals, including those committing crimes, used mobile devices, the government’s affidavit still failed to establish “a fair probability that any pertinent individual would have been using a device that feeds into Google’s location-tracking technology.”¹⁷⁶ Judge Mitchell contrasted the government’s conclusory statements about phones linked to Google’s location-tracking services with the more detailed explanations offered by the government in the Northern District of Illinois warrant applications.¹⁷⁷

Finally, with regard to probable cause, Judge Mitchell found fault with the application’s failure to anticipate the number of individuals likely to be included within the geofence.¹⁷⁸ In her view, the probable-cause inquiry is one of relative scale, in which a large amount of information on innocent individuals “lessens the likelihood that the data would reveal a criminal suspect’s identity, thereby weakening the showing of probable cause.”¹⁷⁹

The opinion similarly emphasized a proportionality requirement for particularity,¹⁸⁰ with the court writing that “[t]he particularity requirement is more stringent if the privacy interest is greater.”¹⁸¹ The court found that the government’s application was “missing key information to determine whether the proposed warrant is sufficiently particularized”: The government did not address the public streets and second business contained within the geofence, nor did it “explain the extent to which the geofence, combined with the margin of error, is likely to capture uninvolved individuals from . . . surrounding

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.* at *3.

176. *Id.*

177. *Id.*

178. *Id.* Judge Mitchell noted that this failure “also goes to the particularity requirement, which is intertwined with probable cause.” *Id.*

179. *Id.*

180. *Id.* (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

181. *Id.* (citing *Berger v. New York*, 388 U.S. 41, 56 (1967)).

properties.”¹⁸² Based on these shortcomings, the court held that the government failed to meet its particularity burden.¹⁸³ The opinion also questioned why the government asked for a whole hour of data, especially given that this period was longer than any period requested in the Northern District of Illinois cases.¹⁸⁴ Although the government’s affidavit mentioned three specific times that the suspect was shown on video surveillance, “[t]he proposed geofence’s temporal scope ranges from just before the second [video] sighting to approximately 10 minutes after the suspect fled the scene.”¹⁸⁵ The government’s failure to explain its timing request in relation to these facts, along with the geofence’s broad geographic boundaries, ultimately rendered the request insufficiently particular.¹⁸⁶

The court denied the government’s application without prejudice, and it did not foreclose “the possibility that the government may be able to adequately demonstrate probable cause to support the warrant and articulate that the proposed geofence is sufficiently particular.”¹⁸⁷ But the court firmly stated its demands and the underlying policy considerations, noting that it is “not enough to submit an affidavit stating that probable cause exists for a geofence warrant because, given broad cell phone usage, it is likely the criminal suspect had a cell phone.”¹⁸⁸ “If this were the standard, a geofence warrant could issue in almost any criminal investigation where a suspect is unidentified.”¹⁸⁹

C. Ongoing State and Federal Litigation

The magistrate opinions discussed in the previous Subparts all emerged from *ex parte* proceedings without a defendant. The first geofence-warrant challenges brought by criminal defendants have emerged in the past year. One such challenge is in the U.S. District Court for the Eastern District of Virginia; another is in the San Francisco County Superior Court, a California trial-level state court. In *United States v. Chatrie*, a federal defendant is challenging a geofence warrant that allegedly identified him as an armed bank robber.¹⁹⁰ The

182. *Id.* at *4.

183. *Id.*

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. Indictment at 1-2, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Sept. 17, 2019), 2019 WL 7660960, ECF No. 1; *Chatrie* Motion to Suppress, *supra* note 78, at 1.

geofence warrant covered a mixed residential–commercial area alongside a busy regional highway.¹⁹¹ In addition to the bank that was robbed, the geofence encompassed the entirety of a megachurch housed inside of a converted Costco superstore.¹⁹² Just outside of the geofenced region is a hotel with sixty-eight guest rooms, the occupants of which would have been included in the Google returns if their maps display radii extended beyond a few yards.¹⁹³ The area covered by the geofence was “78,000 square meters, or about 17 acres,” but with the approximate margin of error added, “the effective range was 470,000 square meters, or about 116 acres.”¹⁹⁴

The execution of the *Chatrie* warrant followed the three-step process described in Part I.B above.¹⁹⁵ After the initial data dump, law enforcement repeatedly sought expanded location history “for one hour on either side of the robbery . . . without geographic restriction” for *all* of the devices that Google identified.¹⁹⁶ Recognizing the overbreadth of this request, “Google did not comply until investigators identified a subset of nine users for further scrutiny.”¹⁹⁷ Law enforcement then narrowed the list and requested that Google unmask the owners of three devices.¹⁹⁸

After the defendant sought to suppress the evidence obtained from the geofence warrant, Google filed an amicus curiae brief in support of neither party.¹⁹⁹ The amicus brief revealed previously unknown information about Google’s use of LH (location history) and defended the corporation’s position that law enforcement must obtain a warrant supported by probable cause in order to access LH records.²⁰⁰ Google did not take a position on the validity of the warrant at issue.²⁰¹

191. *Chatrie* Motion to Suppress, *supra* note 78, at 5-6.

192. *Id.* at 6; Jim McConnell, *A Church Is Born Again Inside an Old Costco*, CHESTERFIELD OBSERVER (Feb. 15, 2017), <https://perma.cc/V4GX-ZU2B>.

193. *Chatrie* Motion to Suppress, *supra* note 78, at 6; *Hampton Inn Richmond-Southwest-Hull Street*, HAMPTON, <https://perma.cc/43BQ-FGLG> (archived Oct. 23, 2021); see Affidavit & Search Warrant at 5, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 18, 2019), ECF No. 54-1.

194. *Chatrie* Supplemental Motion to Suppress, *supra* note 108, at 8-9.

195. *Id.* at 1-2.

196. *Id.* at 2.

197. *Id.*

198. *Id.*

199. See *id.*; Motion for Leave to File Amicus Curiae Brief in Support of Neither Party at 1, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 20, 2019), ECF No. 59; Google Amicus Brief, *supra* note 13, at 1-2.

200. See Google Amicus Brief, *supra* note 13, at 2, 5-14.

201. *Id.* at 2.

In *Chatrie*, the probable-cause statement for the geofence warrant emphasized that the unidentified bank robber appeared to use a cell phone prior to the robbery.²⁰² Based on this crime-specific information and generic recitations regarding cell phone use and Google's LH collection, the Chesterfield Circuit Court approved the warrant.²⁰³

In the San Francisco County Superior Court, the criminal defendant in *People v. Dawes* is similarly challenging a geofence warrant that led to his alleged identification as one of four suspects in a home burglary.²⁰⁴ Before a San Francisco magistrate, officials in *Dawes* presented a statement of probable cause that included even less detail than the *Chatrie* affidavit.²⁰⁵ Law enforcement did not even indicate that a cell phone was used during the crime.²⁰⁶ The investigating officer instead asserted, using boilerplate language, that "[b]ased on my training, experience and consulting with other investigators, I know that subjects who commit crimes, including residential burglaries, often uses [sic] their cell phones as a means of communication during the commission of the crime."²⁰⁷ The statement then summarized how cell phones collect users' LH data for storage on Google's servers.²⁰⁸ While litigants await the district court's ruling in *Chatrie* and the evidentiary hearing in *Dawes*, the law governing geofences remains unsettled.

D. Preliminary Takeaways from the Early Litigation

Early litigation surrounding geofence warrants has revealed emerging judicial views, government attitudes toward geofences, and potential arguments for defendants. For example, the government has shown that it is willing to narrow requests or forgo selective expansion and unmasking when pressured by Google or magistrate judges.²⁰⁹

Although it is early to draw conclusions from five magistrate opinions across two federal districts, we briefly note emerging areas of agreement and disagreement. None of the magistrate judges in the Northern District of Illinois or the District of Kansas held that geofences were categorically

202. Affidavit & Search Warrant, *supra* note 193, at 6.

203. *See id.* at 6-8.

204. *Dawes* Motion to Quash & Suppress, *supra* note 81, at 1-2, 6-8.

205. Statement of Probable Cause at 10-11, *People v. Dawes*, No. 19002022 (Cal. Super. Ct. Dec. 4, 2018) (on file with authors). By our calculation, the geofence in *Dawes* covered roughly 14,000 square feet. *See id.* at 11.

206. *See id.* at 8-10.

207. *Id.* at 10.

208. *Id.*

209. *See supra* Parts III.A.2-.3; *see also supra* notes 196-97 and accompanying text.

unconstitutional.²¹⁰ Rather, the magistrates differed as to when and how a geofence can conform to the constitutional requirements of a warrant.²¹¹ A large part of this disagreement concerned whether probable cause must be shown for each device searched or merely for Google’s SensorVault as a whole.²¹²

Views regarding geofence issues will continue to diverge as the above cases progress—and as new ones arise. We turn now to how Supreme Court precedent on probable-cause and particularity requirements might apply to geofence warrants.

IV. Constitutionality of the Initial Data Dump

Our constitutional analysis begins with an evaluation of the first step of geofence-warrant execution: the initial data dump. This Part shows that the government faces difficulty in satisfying probable-cause and particularity requirements at this step because it generally lacks specific knowledge about the crime when it applies for a geofence warrant. We first consider probable cause for geofence warrants in the context of the Supreme Court’s case law regarding checkpoints, area warrants, and searches of people near a crime scene. We then discuss particularity, first examining geofences that include multi-occupancy buildings and then suggesting particularized search protocols for geofence warrants.

A. Probable Cause

When applying for geofence warrants, law enforcement’s support for probable cause often resembles that proffered in the Northern District of Illinois arson investigation, as described in Part III.A.4 above. An unknown suspect committed a crime at a certain location at a certain time; investigators assumed—with no proof—that the perpetrator had a smartphone with him

210. *See supra* Parts III.A–B.

211. *See supra* Parts III.A–B.

212. *Compare In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 750–51 (N.D. Ill. 2020) (noting that where a geofence warrant “cause[s] the disclosure of the identities of various persons,” the government “must satisfy probable cause as to [each of] those persons”), *with In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 355 (N.D. Ill. 2020) (examining whether there is “probable cause that evidence of the crime will be located at Google”), *and In re the Search of Info. That Is Stored at the Premises Controlled by Google, LLC*, No. 21-mj-05064, 2021 WL 2401925, at *2 (D. Kan. June 4, 2021) (stating that the government must “establish probable cause that evidence of the crime will be located at the place searched—that is, Google’s records”). We address this topic further in Part IV.A below.

during the offense; and investigators noted “a reasonable probability that a cell phone, regardless of its make, is interfacing in some manner with a Google application, service, or platform.”²¹³

Geofence warrants are not the first instance of the government selecting a geographic region and searching everything within it. Sometimes, law enforcement has selected an area and searched every person within it.²¹⁴ At other times, it has selected an area and searched every home within it.²¹⁵ Now, law enforcement selects an area and searches every device within it. Fourth Amendment jurisprudence has long grappled with the probable-cause and particularity requirements of these inherently broad searches.

1. Geofences as *Ybarra* searches

The Supreme Court has made clear that an individual’s mere presence near a crime is insufficient to establish probable cause. In *Ybarra v. Illinois*, an informant told police that he observed a bartender in possession of (and potentially selling) heroin.²¹⁶ A judge issued a warrant authorizing the search of the tavern and the bartender.²¹⁷ When officers arrived, they searched not only the tavern but also all customers present, including Ventura Ybarra.²¹⁸

The Court declared the search unconstitutional because the government’s warrant application only alleged probable cause for the bartender and did not assert proof “that any person found on the premises of the Aurora Tap Tavern, aside from [bartender] ‘Greg,’ would be violating the law.”²¹⁹ “Nowhere . . . did the complaint even mention the [bar’s] patrons.”²²⁰ And Ybarra himself, the Court found, gave police “no reason to believe that he had committed, was committing, or was about to commit any offense under state or federal law.”²²¹ The Court noted that “the agents knew nothing in particular about Ybarra, except that he was present, along with several other customers, in a public tavern at a time when the police had reason to believe that the bartender would have heroin for sale.”²²² As the Court held, “a person’s mere propinquity to . . .

213. *In re the Search Warrant Application*, 497 F. Supp. 3d at 356.

214. *See infra* Parts IV.A.1-2.

215. *See infra* Part IV.A.3.

216. 444 U.S. 85, 87-88 (1979).

217. *Id.* at 88.

218. *Id.* at 88-89. Ybarra, as it turned out, was also in possession of heroin. *Id.* at 89.

219. *Id.* at 90.

220. *Id.*

221. *Id.* at 90-91.

222. *Id.* at 91.

criminal activity does not, without more, give rise to probable cause to search that person.”²²³

An individual Google user being searched via geofence is analogous to Ventura Ybarra being searched at the tavern. Like the warrant application in *Ybarra*, a standard geofence-warrant application alleges two things: (1) that someone committed a crime;²²⁴ and (2) that the crime occurred in a certain location. And like a search of all persons present at the Aurora Tap Tavern, a geofence warrant searches all devices within the specified area.

Similar to the *Ybarra* warrant application, which did not “even mention” individuals other than the bartender,²²⁵ a standard geofence-warrant application does not mention any details about individuals other than the fact that a suspect is likely to be present in the geofence.²²⁶ To borrow from the *Ybarra* Court: The investigators know “nothing in particular about” any individual subjected to the geofence search “except that he was present” in a place “at a time when the police had reason to believe” that a crime occurred.²²⁷

The Court in *Ybarra* underscored that probable cause must be established for each individual subject to the search. The Court’s analysis contrasts with Magistrate Judge Harjani’s reasoning in the Northern District of Illinois arson case discussed above.²²⁸ In granting a geofence warrant, Judge Harjani considered whether there was a fair probability that evidence of the crime would be found *in the SensorVault*, instead of asking whether there was a fair probability that evidence of the crime would be found *in each user account searched*.²²⁹ In reviewing such decisions, courts must grapple with *Ybarra*’s declaration that the probable-cause requirement “cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.”²³⁰

223. *Id.* (citing *Sibron v. New York*, 392 U.S. 40, 62–63 (1968)); *see also* *United States v. Di Re*, 332 U.S. 581, 587 (1948) (holding that an individual does not lose constitutional immunities from search by “mere presence in a suspected car”). This holding applies when presence at a crime scene is a known certainty—but presence is not a certainty with geofence returns because of the way that Google collects data. *See supra* notes 73–77 and accompanying text.

224. But in the geofence case, there is not even a named suspect like “Greg” the bartender.

225. *Ybarra*, 444 U.S. at 90.

226. *See, e.g., supra* notes 202–08 and accompanying text.

227. *Ybarra*, 444 U.S. at 91.

228. *See supra* Part III.A.4.

229. *See In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 355 (N.D. Ill. 2020).

230. *Ybarra*, 444 U.S. at 91.

The analogy, of course, is imperfect. The search of a person in a bar is not the same as the search of a device's location history in a geofenced region. Individuals' privacy preferences differ. Some might feel that it is more privacy invasive for a law enforcement to rifle through pockets or a purse than it is for law enforcement to rifle through location data over the course of an hour. Nevertheless, there are good reasons to think that both physical and geofence searches fall within the same category of Fourth Amendment protection. The search of a cell phone's data generally requires a warrant,²³¹ as does the search of a home.²³² Similarly, the search of cell-site location information generally requires a warrant,²³³ as does the search of a bar patron's pockets.²³⁴ All told, the *Ybarra* search parallels geofence searches for purposes of Fourth Amendment jurisprudence. And *Ybarra* models the analysis a court should employ when evaluating probable cause to conduct searches of many people—or many people's devices.

2. Geofences as checkpoints

Geofence warrants also resemble checkpoints: Both geofences and checkpoints delineate a geographic region and search everyone within that region. The Supreme Court's checkpoint doctrine is illustrated in *Michigan Department of State Police v. Sitz*, in which law enforcement constructed a checkpoint for drunk driving:

All vehicles passing through a checkpoint would be stopped and their drivers briefly examined for signs of intoxication. In cases where a checkpoint officer detected signs of intoxication, the motorist would be directed to a location out of the traffic flow where an officer would check the motorist's driver's license and car registration and, if warranted, conduct further sobriety tests. Should the field tests and the officer's observations suggest that the driver was intoxicated, an arrest would be made.²³⁵

A geofence search is essentially a digitized version of the *Sitz* checkpoint. All devices that passed through the specified region during the relevant time window are revealed in the initial data dump, and their location history is examined by law enforcement for signs of criminal activity. When an officer sees suspicious location history, that individual is selected for further investigation via the selective-expansion step.²³⁶ Should the officer's further observations suggest that the individual is a suspect, the geofence warrant

231. *Riley v. California*, 573 U.S. 373, 386, 401 (2014).

232. *Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990).

233. *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).

234. *Ybarra*, 444 U.S. at 88-89, 90-91.

235. 496 U.S. 444, 447 (1990).

236. *See supra* Part I.B.2.

requires Google to unmask that person and produce his or her subscriber information.²³⁷ In other words, all individuals in the area are preliminarily inspected and, at the officer's discretion, searched. More broadly, law-enforcement officials executing a geofence warrant develop probable cause to investigate certain individuals only *after* they have reviewed the initial data dump (and perhaps selective-expansion data).

The *Sitz* Court found the checkpoint constitutional because it “was clearly aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways, and there was an obvious connection between the imperative of highway safety and the law enforcement practice at issue.”²³⁸ But in *City of Indianapolis v. Edmond*, the Court held that a checkpoint was unconstitutional because its “primary purpose . . . [was] the interdiction of narcotics” and made clear that general-purpose checkpoints are prohibited.²³⁹ The *Edmond* Court declined to “suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes.”²⁴⁰ If such checkpoints were allowed, the Court reasoned, “there would be little check on the ability of the authorities to construct roadblocks for almost any conceivable law enforcement purpose.”²⁴¹ Under this logic, geofence warrants used to investigate ordinary crimes (i.e., those that do not pose an immediate hazard) seem to run afoul of *Edmond* and *Sitz*.

Illinois v. Lidster presents an apt comparison to geofence warrants, as the case involved a criminal investigation in search of leads.²⁴² Faced with a stale investigation of a fatal hit-and-run, law enforcement created an “information-seeking” checkpoint near the accident's location.²⁴³ The checkpoint blocked a portion of the highway so that officers could approach each vehicle, ask passengers if they had witnessed the accident, and hand passengers a flyer requesting assistance in identifying the vehicle and driver involved.²⁴⁴ The Supreme Court upheld this checkpoint as constitutional because, unlike the *Edmond* checkpoint, it was not set up primarily to detect evidence of ordinary

237. See *supra* Part I.B.3.

238. *City of Indianapolis v. Edmond*, 531 U.S. 32, 39 (2000) (citing *Sitz*, 496 U.S. at 451).

239. *Id.* at 41 (“We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.”).

240. *Id.* at 44.

241. *Id.* at 42.

242. See 540 U.S. 419, 422 (2004).

243. *Id.* at 422, 424.

244. *Id.* at 422. Respondent Robert Lidster swerved into the checkpoint and nearly collided with it, and was subsequently arrested for driving under the influence. *Id.*

criminal wrongdoing.²⁴⁵ In the Court's eyes, the key distinguishing factor from *Edmond* was that law enforcement in *Lidster* sought information from third parties unlikely to have themselves committed the crime under investigation.²⁴⁶

Like in *Lidster*, law enforcement has no suspect and no known witnesses when requesting a geofence warrant. But a geofence warrant is more like the checkpoint in *Edmond* than the one in *Lidster*. While *Lidster*'s checkpoint was in furtherance of a criminal investigation, it did not aim to "determine whether a vehicle's occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others."²⁴⁷ As the geofence warrants surveyed above indicate, however, the government seeks geofence warrants precisely to reveal unknown perpetrators.²⁴⁸ Inspection of geofence data is thus equivalent to law enforcement stopping each individual leaving an area, demanding his or her digital device, and checking its location history for evidence of a crime. This is precisely what the Fourth Amendment prohibits.²⁴⁹

3. Geofences as area warrants

Geofences are also analogous to area warrants. One commentator defines area warrants as "judicial warrants that specify the location and timing of a search without specifying the persons or objects to be searched."²⁵⁰ In contrast to typical search warrants, an area warrant, such as an administrative warrant or a suspicionless search, "generally cannot provide much detail beyond . . . an address, a stated purpose, and general parameters for a search."²⁵¹ When an area warrant issues, it authorizes the government to search "every person, place, or thing in a specific location . . . based only on a showing of a generalized government interest."²⁵² Such searches are not predicated on

245. *Id.* at 427-28.

246. *Id.* at 423.

247. *Id.*; see also *id.* at 428 (Stevens, J., concurring in part and dissenting in part) ("There is a valid and important distinction between seizing a person to determine whether she has committed a crime and seizing a person to ask whether she has any information about an unknown person who committed a crime a week earlier.").

248. See *supra* Part II; see also, e.g., *supra* notes 46-48 and accompanying text.

249. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.").

250. Christopher Lee, Comment, *The Viability of Area Warrants in a Suspicionless Search Regime*, 11 U. PA. J. CONST. L. 1015, 1019 (2009).

251. *Id.* at 1044.

252. Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 263 (2011).

probable cause for each thing searched within the specific location,²⁵³ so they cannot meet the usual standard required for warrants. Instead, the Supreme Court recognizes an exception for area warrants in cases where “requiring individualized showings of probable cause would prevent the government from addressing important health or safety concerns,” such as the need to conduct “[a] health or safety inspection of every home in a given area or every business in a particular industry.”²⁵⁴ Because of this unique government rationale, these warrants can be predicated on *sui generis* area-wide probable cause.

The Supreme Court defined the constitutional limits of area warrants in *Camara v. Municipal Court*, which concerned a municipal government’s inspection of housing “based on its appraisal of conditions in the area as a whole, not on its knowledge of conditions in each particular building.”²⁵⁵ In *Camara*, the government expected that many homes subject to search would be in compliance with housing codes.²⁵⁶ As a result, the government’s inspections “would burden many law-abiding homeowners who had done nothing to trigger any suspicion of wrongdoing.”²⁵⁷ Under ordinary Fourth Amendment jurisprudence, such inspections would be prohibited. The *Camara* Court, however, recognized an exception to the usual probable-cause requirement “because the inspections are neither personal in nature nor aimed at the discovery of evidence of crime,” meaning that “they involve a relatively limited invasion of the urban citizen’s privacy.”²⁵⁸

But the Court emphasized that “the importance of the government’s interest” in regulating health and safety and the “minimally intrusive nature of the search” were not, by themselves, sufficient to exempt housing inspections from the requirement of individualized suspicion.²⁵⁹ The Court included in its test an exhaustion requirement, indicating that area warrants were only to be used as a last resort²⁶⁰ and explaining the “unanimous agreement among those most familiar with this field that the *only* effective way to seek universal compliance with the minimum standards required by municipal codes is through routine periodic inspections of all structures.”²⁶¹ The Court

253. *Id.*

254. *Id.* at 262-63.

255. *See* 387 U.S. 523, 535-36 (1967).

256. *Primus, supra* note 252, at 264.

257. *Id.*; *see Camara*, 387 U.S. at 532-33 (emphasizing various ways in which administrative inspections burden each individual whose property is searched).

258. *Camara*, 387 U.S. at 537.

259. *Primus, supra* note 252, at 264.

260. *See Camara*, 387 U.S. at 539-40.

261. *Id.* at 535-36 (emphasis added).

emphasized that no home-inspection technique based on probable cause “would achieve acceptable results,”²⁶² and in the decade after *Camara* it struck down “many proposed administrative searches—even minimally intrusive ones—because alternative regimes predicated on individualized suspicion could reasonably serve the government’s interests.”²⁶³

The *Camara* test thus guides the analysis of whether geofence warrants are permissible area warrants. Instead of inspecting each home in an area based on the probability of housing code violations, geofence warrants allow law enforcement to inspect every digital device in an area based on the likelihood of evidence being found on a device. Many, if not most, devices with information returned will be unrelated to the investigation; many law-abiding people who did nothing to trigger suspicion of wrongdoing will be burdened. The Court in *Camara* made clear that such a search is only permissible in the context of an important public health and safety issue when no other investigative method would suffice.²⁶⁴ Given this analysis, it seems unlikely that a geofence warrant, outside of a special situation or a dire exigency, could pass the high *Camara* bar.

4. Takeaways

As seen through the *Ybarra* opinion and the other examples discussed in the previous Subparts, the probable-cause requirement is likely the main barrier to the constitutionality of geofence warrants. Geofence-warrant applications in their current form assert only that individual users (1) were at or near the scene of a crime; and (2) possessed a cell phone that sends data to Google.²⁶⁵ This falls short of probable cause.

The first allegation, that a user was near the scene of the crime, clashes with *Ybarra*. In order to obtain a geofence warrant, the government may have to show—also in line with the Supreme Court’s checkpoint and area-warrant jurisprudence—that a special need beyond general law-enforcement activity, such as the risk of harm to public health or safety, is present.

The second allegation, that the user has a cell phone which sends data to Google, also seems to fall short of the *Ybarra* hurdle. Owning an iPhone or an Android phone is not a reason to believe that the individual “had committed, was committing, or was about to commit any offense under state or federal law,” and it is not “indicative of criminal conduct.”²⁶⁶ Rather, it is indicative of

262. See *id.* at 537.

263. Primus, *supra* note 252, at 265–66.

264. *Camara*, 387 U.S. at 535–40.

265. See, e.g., *supra* notes 160–61 and accompanying text.

266. *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

living in the twenty-first century and having the means to afford a smartphone.

Prior to receiving geofence-warrant data, investigators have no idea which individuals to scrutinize. All are treated as suspects on the basis of their devices' proximity to the crime scene. While probable cause is merely "a fair probability that contraband or evidence of a crime will be found in a particular place,"²⁶⁷ that place cannot be an entire geographic region. Rather, the place must be each individual device caught in the net. The Constitution requires a basis for suspicion of an individual's wrongdoing, and this basis must go beyond naming an entire population or a blanket geographic region. Indeed, the Constitution requires that probable cause be established for *every individual* whose information is ensnared in the search, and probable cause cannot be satisfied by claiming that evidence of wrongdoing will likely appear in a general pool of data.²⁶⁸ An affidavit merely showing that a crime took place in a certain geographic region at a certain time, while apparently acceptable to some courts, is constitutionally insufficient. And to the extent that courts have found this rationale adequate to issue geofence warrants, we disagree.

This is not the first time courts have used erroneous probable-cause analysis in the context of broad database searches. In a leading opinion on tower dumps,²⁶⁹ *United States v. James*, the court held that probable cause was met because "there was a fair probability that data from the cellular towers in the area of the crimes," rather than data from each cellular device in the area, "would include cellular data related to the individual responsible for the robberies being investigated."²⁷⁰ Stephen Henderson has explained, however,

267. *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

268. See *Marks v. Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996) (holding that "a warrant to search 'all persons present' for evidence of a crime may only be obtained when there is reason to believe that all those present will be participants in the suspected criminal activity," and explaining that such a warrant is only appropriate for a locale "dedicated exclusively to criminal activity"); *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) ("[A]n 'all persons' warrant can pass constitutional muster if the affidavit and information provided to the magistrate supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity.").

269. Tower dumps and geofences share some similarities. A tower dump occurs when law enforcement asks a cell-service provider to produce the phone numbers of every device connected to a certain cell tower during a certain time period, usually near the scene of a crime when the crime was occurring. See Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (Mar. 27, 2014, 11:58 AM), <https://perma.cc/GL7N-SBR5>. The main differences between tower dumps and geofences are (1) that the SensorVault produces more precise location data than cell towers; and (2) that a tower-dump database search is narrower because providers can search one cell tower only. Google Amicus Brief, *supra* note 13, at 10-12, 14.

270. No. 18-cr-00216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019). Despite being an unpublished district court opinion, *James* is a leading opinion because it is one of the

footnote continued on next page

that focusing probable cause on the group rather than the individual “would mean that a larger database is always to be preferred” by law enforcement, because “by definition there will be evidence of crime in that larger set.”²⁷¹ This would lead to an “absurd” understanding of probable cause, Henderson argues: “[A] prosecutor confident that a bank customer is committing tax fraud could access the combined records of *all* customers of that bank because, somewhere in there, she is very sure is evidence of crime.”²⁷² Instead, Henderson asserts, it must be the case that probable cause is required for “each person’s obtained records” in a tower dump, “meaning here each phone number contained within the dump.”²⁷³ Indeed, the Supreme Court in *Camara* explained that while “in a criminal investigation, the police may undertake to recover specific stolen or contraband goods . . . public interest would hardly justify a sweeping search of an entire city conducted in the hope that these goods might be found.”²⁷⁴ “Consequently, a search for these goods, even with a warrant, is ‘reasonable’ only when there is ‘probable cause’ to believe that they will be uncovered in a particular dwelling.”²⁷⁵

B. Issues with the Particularity Requirement

The Fourth Amendment mandates that the description within a search warrant identify the “specific place for which there is probable cause to believe that a crime is being committed,”²⁷⁶ to ensure that searches “will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.”²⁷⁷ Even if there is probable cause to search some users, geofence

few post-*Carpenter* opinions to address the constitutionality of tower dumps. See Shane Rogers, *Two Years of Carpenter*, COVINGTON: INSIDE PRIV. (July 7, 2020), <https://perma.cc/9A8M-CXXS>. Many of our arguments in this Part also apply to tower dumps. Individuals are swept into tower dumps for the same reason they are swept into geofences: proximity to the scene of the crime around the time when it occurred. But the *Carpenter* question is more relevant to tower-dump litigation than to geofence litigation, as corporations sometimes supply cell-tower information to law enforcement without a warrant. David Kravets, *Cops and Feds Routinely “Dump” Cell Towers to Track Everyone Nearby*, WIRED (Dec. 9, 2013, 5:15 PM), <https://perma.cc/KX4W-EPQW>.

271. Stephen E. Henderson, Response, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. SEE ALSO 28, 40-41 (2016).

272. *Id.* at 41.

273. *Id.*

274. *Camara v. Mun. Ct.*, 387 U.S. 523, 535 (1967).

275. *Id.*

276. *United States v. Hinton*, 219 F.2d 324, 326 (7th Cir. 1955).

277. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

warrants—which do not target a specific user or set of users²⁷⁸—struggle to achieve particularity because they do not describe a place for which there is probable cause to search *all* devices present.

Imagine a housing structure for which there is an ordinary, in-person search warrant. When a single warrant covers such an area, including more than one living unit in a multi-occupancy structure (or multiple single-occupancy structures), courts require “adequate probable cause for [the] search of *each* place.”²⁷⁹ This is not an easy showing: As Wayne LaFave explains, it generally “requires a rather special set of facts.”²⁸⁰ For example, “a generalized statement that a person involved in criminality has ‘control’ of the entirety of a multiple-occupancy structure will not suffice.”²⁸¹

As noted above, geofence searches often include multi-occupancy structures within their boundaries. Yet law enforcement has not always adhered to the particularity standard required for such searches. Magistrate Judge Weisman noted this defect in his rejection of the initial pharmaceutical geofence application, writing that the government’s “inclusion of a large apartment complex in one of its geofences raises additional concerns” because it would allow the government to “obtain location information as to an individual who may be in the privacy of their own residence without any showing of probable cause related to that individual or her residence.”²⁸² Such information is invasive: Location data can reveal which room of a person’s home she is in, who is in the home with her, and more.²⁸³

278. In fact, one of the most infamous national security laws, section 702 of the Foreign Intelligence Surveillance Act, *see* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881a), requires more targeting than geofences do. Under this law, the government must task a “selector” to a provider, meaning that the government must provide an “account identifier such as an email address or telephone number,” and then the provider must disclose certain communications to or from that selector. U.S. DEP’T OF COM., U.S. DEP’T OF JUST. & U.S. OFF. OF THE DIR. OF NAT’L INTEL., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCs AND OTHER EU LEGAL BASES FOR EU–U.S. DATA TRANSFERS AFTER *SCHREMS II*, at 7-8 (2020), <https://perma.cc/L4NX-AQYB>.

279. *State v. Ferrari*, 460 P.2d 244, 248 (N.M. 1969) (emphasis added).

280. 2 LAFAVE ET AL., *supra* note 116, § 3.4(e) n.89.

281. *Id.*; *see* *United States v. Clark*, 638 F.3d 89, 94-96 (2d Cir. 2011).

282. *In re the Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-00297, 2020 WL 5491763, at *5 n.7 (N.D. Ill. July 8, 2020) (citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

283. *See supra* notes 33-34 and accompanying text (detailing the precision of SensorVault location information). In 2020, Google released reports analyzing location data to show how COVID-19 had changed movement patterns (and whether people were complying with stay-at-home orders). Casey Newton, *Google Uses Location Data to Show Which Places Are Complying with Stay-at-Home Orders—and Which Aren’t*, VERGE (Apr. 3, 2020, 2:00 AM EDT), <https://perma.cc/QAT6-JNFX>. Such reports reveal the precision with which Google chronicles users’ movements.

It is possible for law enforcement to cleverly craft a search protocol to make it sufficiently particularized. In fact, in the third denial of the pharmaceutical geofence application, Magistrate Judge Fuentes suggested that while law enforcement might not have probable cause for everyone present at *each* geofenced crime scene, it might have probable cause for everyone present at *all* (or multiple) geofenced crime scenes.²⁸⁴ Law enforcement could have requested that Google return only location information for devices that registered LH in two or three geofences. At least one office adopted this approach in an investigation: In August 2018, police officers in Maine asked Google to return information only on users whose data appeared in more than one of the requested locations.²⁸⁵ When crafted in this way—with returns limited to devices recorded across multiple geofences in the case of multiple crime scenes—geofence warrants may be sufficiently particularized.

V. Constitutionality of Selective Expansion and Unmasking

Many geofence warrants authorize a second step, selective expansion, through which law-enforcement officials identify and seek additional information on individual devices from the original data pool.²⁸⁶ Selective expansion can include location history from outside of the geofence's initial location and time boundaries.²⁸⁷ In the subsequent, final step, law-enforcement officials require the targeted provider (so far, primarily Google) to unmask the identity of individuals in the data pool.²⁸⁸

These two steps can be interpreted as violative in several ways. Both selective expansion and unmasking grant executive officers unconstitutional discretion in the execution of a warrant. Furthermore, the selective-expansion step can be viewed as allowing officers to go beyond the specified scope of the warrant. Alternatively, the selective-expansion step can be viewed as authorizing additional (and wholly invalid) separate searches under a single warrant.

A. Geofences as General Warrants

By authorizing multiple steps that are entirely subject to the direction of law enforcement, geofence warrants may grant officers unconstitutional

284. *In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 755-56 (N.D. Ill. 2020).

285. Brewster, *supra* note 67; Mak, *supra* note 83.

286. *See supra* Part I.B.2.

287. *See supra* Part I.B.2.

288. *See supra* Part I.B.3.

discretion in warrant execution. As the Supreme Court wrote in *Marron v. United States*, “[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible.”²⁸⁹ “As to what is to be taken,” the Court noted, “nothing is left to the discretion of the officer executing the warrant.”²⁹⁰

In striking down the general warrant at issue in the foundational English case *Wilkes v. Wood*, the Court of King’s Bench held that undue discretion was left to the King’s officers when they were instructed to “apprehend[] the authors, printers and publishers” of a radical newspaper.²⁹¹ The warrant allowed the officers discretion to search homes of their choosing and seize anything they deemed relevant.²⁹² The *Wilkes* court condemned the warrant because of the “discretionary power” it gave officials in deciding where to search and what to take.²⁹³

The U.S. Supreme Court enshrined the lessons of *Wilkes* and a contemporaneous English case, *Entick v. Carrington*,²⁹⁴ in its canonical Fourth Amendment decision, *Boyd v. United States*.²⁹⁵ The Court subsequently held that particularity is required for electronic searches, finding in *Berger v. New York* that a general wiretap granted “the officer a roving commission to ‘seize’ any and all conversations.”²⁹⁶ Without “adequate judicial supervision or protective procedures,” an electronic search lacking probable cause and particularity, “[a]s with general warrants . . . leaves too much to the discretion of the officer executing the order.”²⁹⁷

Like general warrants, geofence warrants grant discretion to the executing law-enforcement officials. Officers can select users of their choosing and seize (through selective expansion or unmasking) further data from those users without judicial oversight.²⁹⁸ The officers do not name these individuals in advance, nor do they provide affidavits specifying their justifications for selecting certain individuals.²⁹⁹

289. 275 U.S. 192, 196 (1927).

290. *Id.*; see *Arizona v. Gant*, 556 U.S. 332, 345 (2009) (“[T]he central concern underlying the Fourth Amendment . . . [is] the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.”).

291. (1763) 98 Eng. Rep. 489, 496, 498; Lofft 1, 14, 18.

292. See *id.* at 498, Lofft at 18.

293. *Id.*

294. (1765) 95 Eng. Rep. 807; 2 Wils. K.B. 275.

295. 116 U.S. 616, 625-27 (1886).

296. 388 U.S. 41, 58-59 (1967).

297. *Id.* at 59-60.

298. See *supra* Parts I.B.2-.3.

299. *Cf. United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007) (holding that a warrant authorizing the seizure of “any and all data” from a ship’s computer was

footnote continued on next page

In its *Chatrie* briefing, the government argued that geofence-warrant discretion merely enabled officers to acquire *less* information than the constitutional maximum.³⁰⁰ The government analogized its geofence warrant to the Playpen warrant, which allowed the FBI to search the computers of everyone who logged into Playpen, a site on the dark web for child sexual-abuse material, for thirty days.³⁰¹ In a Playpen case before the First Circuit, the court found that the warrant was sufficiently particular and allowed law enforcement to deploy the search “more discretely against particular users.”³⁰² Geofence warrants, however, can be distinguished from the Playpen warrant: The particularity requirement is more easily satisfied for seizures of contraband.³⁰³ This was the case for the Playpen warrant, as the users who accessed contraband on the website provided an adequate basis for probable cause to search their devices.³⁰⁴ By contrast, being in the vicinity of a crime scene is neither contraband nor sufficient to support probable cause on its own.³⁰⁵

B. Selective Expansions as Increases in Scope

The selective-expansion step may also be interpreted as an increase in the warrant’s scope without magistrate approval. Once the constitutional requirements of probable cause and particularity are met, the descriptions in a warrant are critical in limiting the resulting search.³⁰⁶ For example, under a warrant particularized to a building’s first floor, authorities cannot search higher floors.³⁰⁷ Even if the government specifies a selective-expansion protocol, a geofence warrant still only describes the data within its original

an invalid general warrant, as it gave executing officers total discretion as to what they would seize (quoting the warrant)).

300. See Government’s Response in Opposition to Defendant’s Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant at 19-20, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Nov. 19, 2019), 2019 WL 8227160, ECF No. 41 [hereinafter *Chatrie* Government’s Response].

301. *Id.*

302. *United States v. Anzalone*, 208 F. Supp. 3d 358, 363, 368 (D. Mass. 2016) (quoting the warrant’s affidavit), *aff’d*, 923 F.3d 1 (1st Cir. 2019).

303. 2 LAFAYETTE ET AL., *supra* note 116, § 3.4(f); see *United States v. Jenkins*, 680 F.3d 101, 106-07 (1st Cir. 2012) (holding that probable cause to believe contraband will be found in a certain place can satisfy the particularity requirement).

304. See *Anzalone*, 208 F. Supp. 3d at 368; *Chatrie* Government’s Response, *supra* note 300, at 20.

305. See *supra* Part IV.A.1.

306. 2 WAYNE R. LAFAYETTE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.10 (West 2021).

307. *Id.* § 4.10(a).

geographic coordinates and time frame. Searching data outside of those parameters is therefore outside the scope of the warrant, like searching the second floor of an apartment building when a search has only been authorized on the first floor.

Issues with searches beyond the scope of a warrant have arisen frequently in digital Fourth Amendment cases, in part because law enforcement can easily exceed specified bounds when accessing large pools of data. For example, in *United States v. Carey*, the Tenth Circuit held that a police officer searching for evidence of drug trafficking on a computer exceeded a warrant's scope when he clicked through picture files looking for evidence of child sexual-abuse material.³⁰⁸ The court noted that "until he opened the first JPG file," the officer stated "he did not suspect he would find child pornography."³⁰⁹ But once he saw the first image and developed probable cause to believe he would find more like it, the officer could not go searching through the computer without returning to a magistrate for another search warrant.³¹⁰

As *Carey* illustrates, law-enforcement officers do not have probable cause to search any location data beyond the initial data dump until they have surveyed the data in that dump. And like in *Carey*, even when law-enforcement officers have developed probable cause to believe they will find more incriminating evidence in a certain user's location history, they may not be allowed to search through data outside of the original parameters (by requesting expansion from Google) until they receive further judicial authorization.

C. Multiple Searches

Going a step further, recent federal appellate opinions indicate that selective expansion could be interpreted as a violation of the Fourth Amendment maxim that several searches cannot be authorized by one warrant. In *Marron*, the Supreme Court explained that the particularity requirement "prevents the seizure of one thing under a warrant describing another."³¹¹ A warrant "authorizes only one search,"³¹² and "if a place is to be searched a second time the proper procedure is to obtain a second warrant based on an affidavit explaining why there is now probable cause notwithstanding the execution of the earlier warrant."³¹³

308. 172 F.3d 1268, 1272-73 (10th Cir. 1999).

309. *Id.* at 1273.

310. *Id.*

311. *Marron v. United States*, 275 U.S. 192, 196 (1927).

312. *United States v. Keszthelyi*, 308 F.3d 557, 568-69 (6th Cir. 2002).

313. 2 LAFAVE ET AL., *supra* note 116, § 3.4(j).

The multiple steps of the geofence warrant may amount to several searches of user accounts due to the underlying technology. One SensorVault query produces the initial data dump, but once that query is complete and the data has been turned over to law enforcement, a second query is necessary in order to produce the selective-expansion data that law enforcement has requested.³¹⁴

While the Supreme Court has not weighed in on the issue, some courts have held that each query of an electronic database is a search, and multiple queries amount to multiple searches. The Second Circuit recently explained that, in the context of a database containing foreign-intelligence information, each query is a separate search that may require a separate warrant.³¹⁵ Similarly, the Ninth Circuit has held that law enforcement cannot conduct subsequent queries of the information on a computer beyond the initial query authorized by a warrant, because the government “should not be able to comb through [the defendant’s] computers plucking out new forms of evidence that the investigating agents have decided may be useful” after it failed to find all the evidence it would have liked in the initial search.³¹⁶

Geofence warrants authorize exactly what the Ninth Circuit prohibits: They allow the government to comb through Google’s database for additional evidence of wrongdoing after failing to find all of its desired evidence in the initial data dump.³¹⁷ When law enforcement searches data outside of the initially specified time and geographic range, officers may be undertaking multiple searches, an unconstitutional action under a single warrant.

VI. Corporate Policy and Fourth Amendment Protections

Geofence warrants raise questions regarding the role that technology companies play in maintaining Fourth Amendment protections. Relative to the invasive and widespread use of geofences, state and federal legislators have taken little notice of the practice.³¹⁸ And geofence-warrant doctrine is virtually nonexistent in the courts, with no binding precedent as of this writing.³¹⁹ In this void, privacy protections are governed by corporate policy. That Google is regulating state and federal use of geofence warrants has

314. *See supra* Part I.B.2; Google Amicus Brief, *supra* note 13, at 12-14.

315. *United States v. Hasbajrami*, 945 F.3d 641, 669-73 (2d Cir. 2019).

316. *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013).

317. *See supra* Part I.B.2.

318. *See* Issie Lapowsky, *New York Lawmakers Want to Outlaw Geofence Warrants as Protests Grow*, PROTOCOL (June 16, 2020), <https://perma.cc/3HPW-BKT9> (noting that New York’s proposed ban on geofence warrants “would be the first in the United States”).

319. *See supra* Part III.

significant implications for (1) the way that Fourth Amendment analysis is and should be conducted; (2) how user's rights should be protected; and (3) how much deference government litigation positions are owed with regard to geofence surveillance.

This Part begins by discussing the source of the vacuum in which Google has been able to take control: legislative inaction, particularly by the federal government. It then considers (1) Google's reasons for choosing to implement its policies; (2) law enforcement's acquiescence; and (3) the implications of this arrangement on democratic accountability, consumer privacy, and the role of the courts.

A. Absence of Legislation

Legislative rules could govern and regulate the use of geofence warrants, going above the constitutional floor or mandating protections in the absence of a precedential holding.³²⁰ But Congress has displayed little inclination to act. Similarly, although a few promising signs have emerged in certain state legislatures, no bill that would curb geofence use by law enforcement has neared passage.

At the time of writing, Congress has not indicated a willingness to regulate law enforcement's access to geofence data. The only direct mention of geofence warrants in Congress came in a July 2020 appearance by the chief executive officers of Alphabet (Google's parent company), Amazon, Apple, and Facebook before the House Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law.³²¹ During that hearing, Representative Kelly Armstrong explained to Alphabet CEO Sundar Pichai that he believed geofence warrants were "the single most important issue" before the Subcommittee, because such warrants fall short of the Fourth Amendment's probable-cause and particularity requirements.³²² "People would be terrified to know,"

320. Cf. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004) (explaining how the Stored Communications Act created a "set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information"); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 24-26 (2004) (detailing how the Wiretap Act set protections above the constitutional floor after the Supreme Court's decision in *Berger*).

321. See *User Clip: Google "Geofence" Warrants Questioned*, C-SPAN (July 29, 2020), <https://perma.cc/WR4C-66TC>. A 2019 letter to Google from the House Committee on Energy and Commerce also expressed concern about the SensorVault's storage of precise location data. Letter from U.S. House of Representatives Comm. on Energy & Com. Members to Sundar Pichai, Chief Exec. Officer, Google 1-3 (Apr. 23, 2019), <https://perma.cc/JSW7-W9AY>. No response from Google has been reported.

322. *User Clip: Google "Geofence" Warrants Questioned*, *supra* note 321, at 02:06-02:10.

Representative Armstrong emphasized, “that law enforcement can grab general warrants and get everybody’s information anywhere.”³²³

There has been slightly more movement at the state level. In April 2020, legislators in New York’s Assembly and Senate introduced legislation to ban law enforcement’s use of geofence searches.³²⁴ New York’s proposed ban—the first such legislation nationally—would prohibit “the search, with or without a warrant, of geolocation data of a group of people who are under no individual suspicion of having committed a crime.”³²⁵ As of this writing, however, neither bill has advanced out of committee.³²⁶

Some states have their own data privacy regimes that grant additional protections beyond federal requirements. For example, California’s Electronic Communications Privacy Act (CalECPA) generally requires a warrant to access “electronic device information” regardless of who possesses the data.³²⁷ Other states, including Maine,³²⁸ Massachusetts,³²⁹ Minnesota,³³⁰ Montana,³³¹ New Hampshire,³³² Rhode Island,³³³ Utah,³³⁴ and Vermont³³⁵ have similar judicial or statutory requirements for a warrant to obtain digital location

323. *Id.* at 01:56-02:00.

324. Assemb. 10246-A, 243d Leg., Reg. Sess. (N.Y. 2020), <https://perma.cc/8BQJ-VF79>; S. 8183, 243d Leg., Reg. Sess. (N.Y. 2020), <https://perma.cc/M4Z7-L7QB>.

325. N.Y. Assemb. 10246-A; N.Y.S. 8183; Lapowsky, *supra* note 318; *see also* Uberti, *supra* note 30; Mike Maharrey, *New York Bill Would Ban Geolocation Tracking and Geofencing Warrants*, TENTH AMEND. CTR. (Apr. 15, 2020), <https://perma.cc/M2YD-J4F4>; Press Release, Surveillance Tech. Oversight Project, S.T.O.P. Welcomes Introduction of NY Geolocation Tracking Ban (Apr. 10, 2020), <https://perma.cc/4A7E-2FPY>.

326. *Assembly Bill A10246A*, N.Y. ST. SENATE, <https://perma.cc/6YSR-WXWN> (archived Oct. 23, 2021); *Senate Bill S8183*, N.Y. ST. SENATE, <https://perma.cc/DV9L-USFT> (archived Oct. 23, 2021). Another bill in Utah that would have placed some limits on the use of geofence warrants gained traction in 2021 but ultimately did not pass. H.R. 251, 64th Leg., 2021 Gen. Sess. (Utah 2021), <https://perma.cc/C63U-97KH>; *H.B. 251 Electronic Location Amendments*, UTAH ST. LEGISLATURE, <https://perma.cc/248V-5MGJ> (archived Jan. 29, 2022); Art Raymond, *Bill Targets How Police Use Info Showing Where You’ve Been and What Internet Searches You Make*, DESERET NEWS (Feb. 25, 2021, 9:52 PM MST), <https://perma.cc/4SYU-L96F>.

327. CAL. PENAL CODE §§ 1546(g), 1546.1(c) (West 2021).

328. ME. REV. STAT. ANN. tit. 16, § 648 (2021).

329. *Commonwealth v. Augustine*, 4 N.E.3d 846, 863-66 (Mass. 2014).

330. MINN. STAT. § 626A.42 subd. 2 (2021).

331. MONT. CODE ANN. § 46-5-110 (2021).

332. N.H. REV. STAT. ANN. § 644-A:2 (2021).

333. 12 R.I. GEN. LAWS § 12-32-2 (2021).

334. UTAH CODE ANN. § 77-23c-102 (West 2021).

335. VT. STAT. ANN. tit. 13, §§ 8101, 8102 (2021).

information.³³⁶ Warrants governed by CalECPA must include the “time periods covered,” the “applications or services covered, and the types of information sought,” and they must “describe with particularity the information to be seized by specifying . . . the target individuals or accounts.”³³⁷ CalECPA’s particularity requirement was briefed in *Dawes* as independent grounds to invalidate the warrant.³³⁸ It is not yet clear, however, whether existing state privacy laws can address the concerns of geofence warrants. And many states lack data privacy regimes altogether.

B. Corporate Constitutional Policy

Because of legislative inaction, private corporate policy has replaced democratic governance for geofence warrants. When judges consider geofence warrants, they should therefore note that what comes before them is not the product of democratically considered legislation, but rather the result of internal policy decisions by a single corporation, Google, with which law enforcement has complied.³³⁹

Early geofence warrants sought subscriber information and location history for all devices within the geofence—essentially an unrestrained,

336. See generally *State Location Privacy Policy*, ELEC. PRIV. INFO. CTR., <https://perma.cc/55CU-JSWK> (archived Oct. 23, 2021) (tracking pending and passed state legislation focused on location privacy); *Cell Phone Privacy*, ACLU, <https://perma.cc/2D6E-VE6Y> (archived Oct. 23, 2021) (highlighting the ACLU’s various efforts to increase cell phone users’ privacy rights). For those users willing to proactively limit what location (and other personal) data is held by mobile carriers and technology corporations, the California Consumer Privacy Act (CCPA) protects any personal information that “identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,” including geolocation data. CAL. CIV. CODE § 1798.140(o)(1) (West 2021). Under the CCPA, an individual can find out what types of personal data a business has collected and how such information is to be used. Individuals can also direct businesses to (1) delete their personal information if certain conditions are met; or (2) refrain from selling their data to third parties. *Id.* §§ 1798.100, .105, .110, .115, .120, .130, .135.

337. CAL. PENAL CODE § 1546.1(d)(1) (West 2021).

338. See *Dawes* Motion to Quash & Suppress, *supra* note 81, at 16–19. CalECPA, in contrast to similar federal laws, includes a statutory suppression remedy. Compare PENAL § 1546.4(a), with 18 U.S.C. §§ 2703, 2708.

339. This Subpart’s discussion builds on literature examining (1) how a lack of legislation can affect the exercise of constitutional rights; and (2) the role of corporations in this context. See generally Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 575–78, 653–54 (2018) (noting that law enforcement increasingly uses unregulated hacking technology to access encrypted computer systems); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1601–03 (2018) (exploring how private platforms’ policies increasingly control public debate, free speech, and democratic norms).

unmasked data dump.³⁴⁰ In response to these broad requests, Google adopted an internal policy of objecting to any request that was not a probable-cause search warrant.³⁴¹ It also created the current three-step process in an effort to narrow the amount of identifying information produced.³⁴² Without judicial or legislative action, Google essentially imposed a warrant requirement and ex ante search protocols. The corporation even filed an amicus brief in *Chatrie* asserting that its own policy should be the constitutional minimum.³⁴³

And law enforcement has deferred to Google's policy. Consequently, most affidavits accompanying geofence warrants are boilerplate, sharing the same multistep form and general supporting statements.³⁴⁴ Law enforcement has apparently decided that it is better to avoid litigation against well-resourced Google and not challenge its policy.

Google's power in the geofence-warrant process parallels the larger social and political power of technology companies. As Alan Rozenshtein writes, "[b]y entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of surveillance intermediaries: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance."³⁴⁵ In recent years, these surveillance intermediaries have increasingly challenged subpoenas and search warrants; commentators have tied this change to consumer privacy concerns after Edward Snowden's 2013 surveillance disclosures.³⁴⁶ In one notable instance, Microsoft invoked its duty to its customers when it sued the federal government over the routine inclusion of secrecy orders alongside search warrants.³⁴⁷ The threat of Google litigating in

340. Declaration of Sarah Rodriguez, *supra* note 10, ¶ 5.

341. See, e.g., Affidavit ¶ 1 n.1, *In re the Search of Info. Regarding Accts. Associated With Certain Location and Date Info.*, No. 18-mj-00169 (W.D. Tex. Jan. 10, 2019), ECF No. 9-1 ("Google has indicated that it believes a search warrant is required to obtain the location data sought in this application.").

342. See Declaration of Sarah Rodriguez, *supra* note 10, ¶ 5.

343. See *supra* notes 199-201 and accompanying text.

344. See, e.g., sources cited *supra* note 80.

345. Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 105 (2018) (emphasis omitted); see also Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600 (2009) ("The prospect of resistance from the legal teams of third-party record holders often creates a substantial deterrence against government overreaching even when the third-party doctrine does not.").

346. See *Developments in the Law—More Data, More Problems*, 131 HARV. L. REV. 1714, 1726-27 (2018) (discussing the rise in litigation "challenging the government over requests for information" since the Snowden revelations).

347. See Brad Smith, *Keeping Secrecy the Exception, Not the Rule: An Issue for Both Consumers and Businesses*, MICROSOFT: MICROSOFT ON THE ISSUES (Apr. 14, 2016), <https://perma.cc/5Z5G-TGF5>.

the geofence context fits into this broader trend.³⁴⁸ But while Google may have post-Snowden economic incentives to consider privacy concerns, it remains a body with little direct accountability. Absent legislation, Google is beholden only to its shareholders and its corporate purpose.

Privacy “on the ground” thus remains the product of corporate norms and private review processes.³⁴⁹ While the European Union has mandated a robust privacy regime under the General Data Protection Regulation (GDPR),³⁵⁰ the United States remains a regulatory patchwork lacking meaningful, binding national privacy requirements.³⁵¹ Without clear standards from legislation, corporations fashion their own protocols and thresholds for responding to subpoenas, warrants, and other law-enforcement requests.³⁵² Democratic oversight is dangerously absent, a shortcoming that even some technology companies are eager to see remedied. As Apple CEO Tim Cook told the

348. See Brewster, *supra* note 67; Rozenshtein, *supra* note 345, at 109 (“Intermediaries couple a proceduralism that rejects voluntary cooperation with government requests to an aggressive litigiousness against government demands for data and restrictions on publicizing those requests.” (emphasis omitted)).

349. See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 261-63 (2011) (describing the rise of corporate privacy audits, privacy certification programs, and chief privacy officers).

350. Council Regulation 2016/679, 2016 O.J. (L 119) 1; see *The EU General Data Protection Regulation: Questions and Answers*, HUM. RTS. WATCH (June 6, 2018, 5:00 AM EDT), <https://perma.cc/M6A3-RYHV> (surveying the GDPR’s various requirements, including consumer consent, special protections for sensitive information, disclosure, privacy by design, and the right to be forgotten).

351. See Michael Beckerman, Opinion, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), <https://perma.cc/RDA7-T8S9> (arguing that federal inaction on data privacy legislation has resulted in “inconsistent treatment of data depending on a variety of factors, including the residency of the consumer and the type of businesses with whom they interact”). The standards that do exist are long outdated, with Congress continually refusing to update the Electronic Communications Privacy Act of 1986 (ECPA), which rests on an understanding of technology that is now obsolete. See *ECPA (Part 1): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 1 (2013) (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary) (“The Electronic Communications Privacy Act of 1986 . . . is complicated, outdated, and largely unconstitutional.”); *id.* at 48 (statement of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.) (“The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2013, ECPA frustrates users’ reasonable expectations of privacy.”); see also Kerr, *supra* note 320, at 1208 (noting that the Stored Communications Act, which forms part of ECPA, “is a bit outdated and has several gaps in need of legislative attention”).

352. The absence of legislation also allows corporations to self-regulate in other realms traditionally protected by the Constitution, including speech. See Klonick, *supra* note 339, at 1615, 1666-69 (describing how moderation by private online platforms shapes U.S. speech norms).

European Parliament, “our own information . . . is being weaponized against us with military efficiency.”³⁵³ “Scraps of data,” Cook noted, “each one harmless enough on its own, are carefully assembled, synthesized, traded, and sold.”³⁵⁴ Accordingly, after he praised “the transformative work of the European institutions tasked with a successful implementation of the GDPR,” Cook voiced Apple’s “full support of a comprehensive federal privacy law in the United States.”³⁵⁵

As it currently stands, corporations are free to shift their privacy policies in response to global events, political currents, and economic incentives. When Apple announced that it planned to scan U.S. iPhones and their encrypted messages for images of child sexual abuse, for example, the Electronic Frontier Foundation decried the decision as “a shocking about-face for users who have relied on the company’s leadership in privacy and security.”³⁵⁶ After this and other backlash, Apple reversed its decision.³⁵⁷

But not all shifts are protective, and some shifts are less protective than others. Although Google has announced the development of a “Privacy Dashboard” for future rollout to Android users,³⁵⁸ this feature will offer fewer tracking protections and consent workflows than Apple’s current iPhone operating system.³⁵⁹ And Android phones, relative to iPhones, are more likely to be owned by poorer consumers.³⁶⁰ As a result, if geofence warrants remain pervasive, those caught up in data returns from Google (or possibly other corporations) will disproportionately be Android users, on the whole a less

353. Eur. Data Prot. Supervisor, *Keynote Address from Tim Cook, CEO, Apple Inc.*, YOUTUBE, at 05:41-05:50 (Oct. 24, 2018), <https://perma.cc/8SAB-ELYW>.

354. *Id.* at 06:15-06:25.

355. *Id.* at 08:11-08:20, 08:52-08:59.

356. India McKinney & Erica Portnoy, *Apple’s Plan to “Think Different” About Encryption Opens a Backdoor to Your Private Life*, ELEC. FRONTIER FOUND. (Aug. 5, 2021), <https://perma.cc/Y7Z4-2SRA>; see Frank Bajak & Barbara Ortutay, *Apple to Scan U.S. iPhones for Images of Child Sexual Abuse*, AP NEWS (Aug. 6, 2021), <https://perma.cc/2WAD-HSUV>.

357. See Carly Page, *Apple Quietly Pulls References to Its CSAM Detection Tech After Privacy Fears*, TECHCRUNCH (Dec. 15, 2021, 6:24 AM PST), <https://perma.cc/P5AC-MKH9>.

358. See Sarah N-Marandi, *What’s New in Android Privacy*, ANDROID DEVS. BLOG (May 18, 2021), <https://perma.cc/4CYN-E6E9>.

359. Gerrit De Vynck, *Google Announces New Privacy Features for Android Phones—but Stops Short of Limiting Ad Tracking*, WASH. POST (May 18, 2021, 8:53 PM EDT), <https://perma.cc/47XW-ZVJ8>.

360. See Press Release, Slickdeals, *iPhone Users Spend \$101 Every Month on Tech Purchases, Nearly Double of Android Users, According to a Survey Conducted by Slickdeals* (Oct. 30, 2018), <https://perma.cc/4JY7-Y9W2>; see also Jim Edwards, *Here’s Why Developers Keep Favoring Apple Over Android*, SLATE (Apr. 4, 2014, 1:23 PM), <https://perma.cc/M5QB-9GE8>.

wealthy group. Absent legislation or executive action, the only chance of addressing such inequities may be through corporate policy.

Given our current regulatory vacuum, the role of courts in assessing geofence warrants is paramount. When a court considers a geofence warrant, there is a danger that it will uncritically rely on whatever information the government presents. Indeed, some commentators have argued that federal magistrates are subject to Department of Justice capture.³⁶¹ If courts uncritically rely on government positions regarding geofence warrants, they are transitively subject to Google capture. Courts must remain vigilant in enforcing the underlying probable-cause and particularity requirements of geofence warrants, and they should not simply rubber-stamp Google's *ex ante* search protocols. While Google's procedures may narrow the scope of a geofence warrant, they do not automatically create a search that is acceptable under the Fourth Amendment. In particular, courts should be skeptical of discretionary selective expansion, where law enforcement returns to and negotiates with Google instead of a magistrate to seek an expanded search.³⁶² Courts cannot unilaterally stop consumer data from being used in a widespread surveillance regime. But they can prevent corporate technology giants from replacing the constitutionally mandated check of a neutral judiciary.

Conclusion

Geofence warrants raise important Fourth Amendment questions. Courts have yet to engage deeply with issues of probable cause, particularity, and search expansion as they relate to geofences. And with corporate procedural demands shaping the legal terrain, law enforcement's tendency toward minimally specific warrants has faced little resistance. Without legislative action or increased judicial scrutiny of geofence warrants, undemocratic, discretionary corporate policy will continue to shape location-history protections.

As a closing note: Many commentators have highlighted the utility of geofence warrants, explaining that they "greatly enhance[] investigations,"³⁶³ "help authorities catch criminals,"³⁶⁴ and so on. These comments may be true,

361. See Mayer, *supra* note 339, at 651 ("In the district courts in particular, federal prosecutors are consummate repeat players The result appears to be a (mild) form of regulatory capture, in which prosecutorial arguments receive unusual deference." (footnote omitted)).

362. See *supra* notes 196-97 and accompanying text.

363. Devon Alan Frankel, *Digital Dragnet: Geofence Warrants and Their Constitutional Issues 1* (2020), <https://perma.cc/8Z32-HD3U>.

364. Wendy Davis, *Law Enforcement Is Using Location Tracking on Mobile Devices to Identify Suspects, but Is It Unconstitutional?*, ABA J. (Dec. 1, 2020, 1:50 AM CST), <https://perma.cc/>
footnote continued on next page

but they miss the point. Geofence warrants are indeed a powerful investigative tool. The same can be said for Carpenter’s cell-site location information,³⁶⁵ the eavesdrop orders placed on Berger’s conversations,³⁶⁶ and the door-to-door search used to find and arrest Wilkes.³⁶⁷ Such is the burden of the Bill of Rights: “Privacy comes at a cost.”³⁶⁸

J2GK-S3JU. Sandra Doorley, president of the District Attorneys Association of the State of New York and a district attorney in Monroe County, noted that geofence warrants have “proven to be helpful in solving crimes such as pattern burglaries, arsons and sexual assaults.” *Id.* (quoting Doorley). As previously discussed, carefully crafted geofence-warrant applications for these pattern crimes could pass constitutional muster. *See supra* notes 284-85 and accompanying text.

365. *See* *Carpenter v. United States*, 138 S. Ct. 2206, 2220-21 (2018) (placing limits on the use of this information).

366. *See* *Berger v. New York*, 388 U.S. 41, 58-59 (1967) (placing limits on the use of this practice).

367. *See* *Wilkes v. Wood* (1763) 98 Eng. Rep. 489, 498-99; Lofft 1, 18-19 (placing limits on the use of this technique).

368. *Riley v. California*, 573 U.S. 373, 401 (2014).